

DOCKET NO.: 252399US6PCT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

IN RE APPLICATION OF: Satoshi KITANI

SERIAL NO.: NEW U.S. PCT APPLICATION

FILED: HERewith

INTERNATIONAL APPLICATION NO.: PCT/JP03/15525

INTERNATIONAL FILING DATE: December 4, 2003

FOR: RECORDING AND REPRODUCING APPARATUS, DATA PROCESSING APPARATUS,
AND RECORDING, REPRODUCING, AND PROCESSING SYSTEM**REQUEST FOR PRIORITY UNDER 35 U.S.C. 119
AND THE INTERNATIONAL CONVENTION**Commissioner for Patents
Alexandria, Virginia 22313

Sir:

In the matter of the above-identified application for patent, notice is hereby given that
the applicant claims as priority:

<u>COUNTRY</u>	<u>APPLICATION NO</u>	<u>DAY/MONTH/YEAR</u>
Japan	2002-355114	06 December 2002

Certified copies of the corresponding Convention application(s) were submitted to the International Bureau in PCT Application No. PCT/JP03/15525. Receipt of the certified copy(s) by the International Bureau in a timely manner under PCT Rule 17.1(a) has been acknowledged as evidenced by the attached PCT/IB/304.

Respectfully submitted,
OBLON, SPIVAK, McCLELLAND,
MAIER & NEUSTADT, P.C.



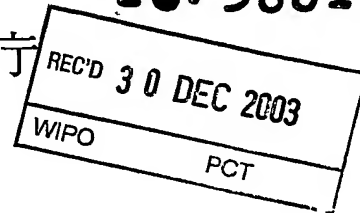
Gregory J. Maier
Attorney of Record
Registration No. 25,599
Surinder Sachar
Registration No. 34,423

Customer Number

22850

(703) 413-3000
Fax No. (703) 413-2220
(OSMMN 08/03)

JP03/15525

04.12.03
500152日本国特許庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出願年月日 2002年12月 6日
Date of Application:

出願番号 特願2002-355114
Application Number:
[ST. 10/C]: [JP2002-355114]

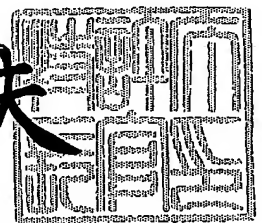
出願人 ソニー株式会社
Applicant(s):

PRIORITY DOCUMENT
SUBMITTED OR TRANSMITTED IN
COMPLIANCE WITH
RULE 17.1(a) OR (b)

2003年 8月22日

特許庁長官
Commissioner,
Japan Patent Office

今井康夫



【書類名】 特許願

【整理番号】 0290684306

【提出日】 平成14年12月 6日

【あて先】 特許庁長官 太田 信一郎 殿

【国際特許分類】 H04N 5/85

【発明者】

 【住所又は居所】 東京都品川区北品川 6 丁目 7 番 3 5 号 ソニー株式会社
 内

 【氏名】 木谷 聡

【特許出願人】

 【識別番号】 000002185

 【氏名又は名称】 ソニー株式会社

【代理人】

 【識別番号】 100082762

 【弁理士】

 【氏名又は名称】 杉浦 正知

 【電話番号】 03-3980-0339

【選任した代理人】

 【識別番号】 100120640

 【弁理士】

 【氏名又は名称】 森 幸一

【手数料の表示】

 【予納台帳番号】 043812

 【納付金額】 21,000円

【提出物件の目録】

 【物件名】 明細書 1

 【物件名】 図面 1

 【物件名】 要約書 1

 【包括委任状番号】 0201252

【プルーフの要否】

要

【書類名】 明細書

【発明の名称】 記録再生装置、データ処理装置および記録再生処理システム

【特許請求の範囲】

【請求項 1】 記録媒体固有の第 1 の情報を保持している記録媒体への暗号化されたデータを記録する記録部および上記記録媒体に記録されている暗号化されたデータを再生する再生部の少なくとも一方と、

正当な電子機器またはアプリケーションソフトウェアにのみ与えられる当該電子機器またはアプリケーションソフトウェア固有の第 2 の情報が格納される格納部と、

上記記録媒体固有の第 1 の情報と上記格納部に格納された第 2 の情報とに基づいて生成された鍵を用いて、データの暗号化および暗号化されたデータの復号の少なくとも一方を行うデータ処理装置と相互認証を行う接続部とを有することを特徴とする記録再生装置。

【請求項 2】 請求項 1 において、

上記第 2 の情報の一部が上記格納部に格納され、上記データ処理装置に格納された他の部分と合成されて上記第 2 の情報が形成されるようにした記録再生装置。

【請求項 3】 請求項 1 において、

少なくとも上記格納部に格納された第 2 の情報と上記記録媒体固有の第 1 の情報とを用いて、当該格納された第 2 の情報が正当な電子機器またはアプリケーションソフトウェア固有の情報でない場合にリボケーションを行うリボーク処理部を有する上記データ処理装置に対して、上記接続部が上記格納部に格納された第 2 の情報を送ることを特徴とする記録再生装置。

【請求項 4】 請求項 3 において、

上記第 2 の情報を暗号化して送る記録再生装置。

【請求項 5】 請求項 1 において、

上記格納部に格納された第 2 の情報と上記記録媒体固有の第 1 の情報とを用いて、当該格納された第 2 の情報が正当な電子機器またはアプリケーションソフトウェア固有の情報でない場合にリボケーションを行うリボーク処理部を有するこ

とを特徴とする記録再生装置。

【請求項 6】 記録媒体固有の第 1 の情報を保持している記録媒体への暗号化されたデータを記録する記録部および上記記録媒体に記録されている暗号化されたデータを再生する再生部の少なくとも一方と、

正当な電子機器またはアプリケーションソフトウェアにのみ与えられる当該電子機器またはアプリケーションソフトウェア固有の第 2 の情報が格納される格納部と、

上記記録媒体固有の第 1 の情報と上記格納部に格納された第 2 の情報とに基づいて生成された鍵を用いて、データの暗号化および暗号化されたデータの復号の少なくとも一方を行うデータ処理装置と相互認証を行う接続部と

少なくとも上記接続部を介して上記データ処理装置から送られ、上記格納部に格納された第 2 の情報と、上記記録媒体固有の第 1 の情報とを用いて、当該格納された第 2 の情報が正当な電子機器またはアプリケーションソフトウェア固有の情報でない場合にリボケーションを行うリボーク処理部を有することを特徴とする記録再生装置。

【請求項 7】 請求項 6 において、

暗号化された上記第 2 の情報を復号する復号手段を有する記録再生装置。

【請求項 8】 正当な電子機器またはアプリケーションソフトウェアにのみ与えられる当該電子機器またはアプリケーションソフトウェア固有の第 2 の情報を有するとともに、記録媒体固有の第 1 の情報を保持している記録媒体への暗号化されたデータの記録および上記記録媒体に記録されている暗号化されたデータの再生の少なくとも一方を行う記録再生装置と相互認証を行う接続部と、

上記接続部を介して上記記録再生装置から送られた、上記記録媒体固有の第 1 の情報と上記電子機器またはアプリケーションソフトウェア固有の第 2 の情報とに基づいて生成された鍵を用いて、データの暗号化および暗号化されたデータの復号の少なくとも一方を行う処理部と

を有することを特徴とするデータ処理装置。

【請求項 9】 請求項 8 において、

上記第 2 の情報の一部が上記格納部に格納され、上記記録再生装置に格納され

た他の部分と合成されて上記第2の情報が形成されるようにしたデータ処理装置。

【請求項10】 請求項8において、

上記接続部を介して上記記録再生装置から送られた上記第2の情報と、上記記録媒体固有の第1の情報とを用いて、上記第2の情報が正当な電子機器またはアプリケーションソフトウェア固有の情報でない場合にリボケーションを行うリボーク処理部を有することを特徴とするデータ処理装置。

【請求項11】 請求項10において、

暗号化された上記第2の情報を復号する復号手段を有するデータ処理装置。

【請求項12】 請求項8において、

少なくとも上記記録再生装置に格納された第2の情報と、上記記録媒体固有の第1の情報とを用いて、当該格納された第2の情報が正当な電子機器またはアプリケーションソフトウェア固有の情報でない場合にリボケーションを行うリボーク処理部を有する上記記録再生装置と接続することを特徴とするデータ処理装置。

【請求項13】 正当な電子機器またはアプリケーションソフトウェアにのみ与えられる電子機器またはアプリケーションソフトウェア固有の第2の情報を有する格納部と、

記録媒体固有の第1の情報を保持している記録媒体への暗号化されたデータの記録および上記記録媒体に記録されている暗号化されたデータの再生の少なくとも一方を行う記録再生装置と相互認証を行う接続部と、

上記記録媒体固有の第1の情報と上記格納部に格納された第2の情報とに基づいて生成された鍵を用いて、データの暗号化および暗号化されたデータの復号の少なくとも一方を行う処理部とを有し、

上記格納部に格納された第2の情報が正当な電子機器またはアプリケーションソフトウェア固有の情報でない場合にリボケーションを行うリボーク処理部を有する上記記録再生装置に対して、上記格納部に格納された第2の情報を送ることを特徴とするデータ処理装置。

【請求項14】 請求項13において、

上記第2の情報を暗号化して送るデータ処理装置。

【請求項15】 記録媒体固有の第1の情報を保持している記録媒体への暗号化されたデータの記録および上記記録媒体に記録されている暗号化されたデータの再生の少なくとも一方が可能であると共に、正当な電子機器またはアプリケーションソフトウェアにのみ与えられる電子機器またはアプリケーションソフトウェア固有の第2の情報を有する記録再生装置と、

少なくとも格納された上記第2の情報と、上記記録媒体固有の第1の情報とに基づいて生成された鍵を用いて、データの暗号化および暗号化されたデータの復号の少なくとも一方を行うデータ処理装置と

を有することを特徴とする記録再生処理システム。

【請求項16】 請求項15において、

上記データ処理装置が上記記録媒体固有の第1の情報と格納された上記第2の情報を用いて、当該格納された第2の情報が正当な電子機器またはアプリケーションソフトウェア固有の情報でない場合にリボケーションを行うリボーク処理部を有することを特徴とする記録再生処理システム。

【請求項17】 請求項15において、

上記記録再生装置が上記記録媒体固有の第1の情報と格納された上記第2の情報を用いて、当該格納された第2の情報が正当な電子機器またはアプリケーションソフトウェア固有の情報でない場合にリボケーションを行うリボーク処理部を有することを特徴とする記録再生処理システム。

【請求項18】 正当な電子機器またはアプリケーションソフトウェアにのみ与えられる当該電子機器またはアプリケーションソフトウェア固有の情報として格納された第2の情報を有するとともに、記録媒体固有の第1の情報を保持している記録媒体への暗号化されたデータの記録および上記記録媒体に記録されている暗号化されたデータの再生の少なくとも一方を行う記録再生装置と、

格納された上記第2の情報と、上記記録媒体固有の第1の情報とに基づいて生成された鍵を用いてデータの暗号化、または暗号化されたデータの復号が可能なデータ処理装置とからなり、

格納された上記第2の情報が正当な電子機器またはアプリケーションソフトウ

エア固有の情報でない場合にリボケーションを行うリボーク処理部を有する上記記録再生装置に対して、上記データ処理装置が上記格納部に格納された第2の情報を送ることを特徴とする記録再生処理システム。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】

この発明は、例えばパーソナルコンピュータと接続されたドライブによってディスクメディアに暗号化コンテンツを記録し、また、ディスクメディアから暗号化コンテンツを再生する場合に適用される記録再生装置、データ処理装置および記録再生処理システムに関する。

【0002】

【従来の技術】

近年開発されたDVD (Digital Versatile Disc またはDigital Video Disc) 等の記録媒体では、1枚の媒体に例えば映画1本分の大量のデータをデジタル情報として記録することが可能である。このように映像情報等をデジタル情報として記録することが可能となると不正コピーを防止して著作権の保護を図ることがますます重要となっている。

【0003】

DVD-Videoでは、コピープロテクション技術としてCSS (Content Scrambling System) が採用されている。CSSは、DVDメディアに対する適用のみが認可されており、DVD-R、DVD-RW、DVD+R、DVD+RW等の記録型DVDでのCSSの利用がCSS契約によって禁止されている。したがって、DVD-Videoの内容を記録型DVDへのまるごとコピー（ビットバイビットコピー）は、CSS契約上では、認められた行為ではない。

【0004】

しかしながら、CSSの暗号方式が破られる事態が発生した。CSSの暗号化を解除してDVD-Videoの内容を簡単にハードディスクにコピーする「DeCSS」と呼ばれる違法なソフトウェアがインターネット上で配布された。「DeCSS」が出現した背景には、本来耐タンパー化が義務付けられているはずの

C S S 復号用の鍵データを耐タンパー化しないまま設計された再生ソフトウェアがリバースエンジニアされて鍵データが解読されたことによって、連鎖的に C S S アルゴリズム全体が解読された経緯がある。

【 0 0 0 5 】

C S S の後に、D V D - Audio等の D V D - R O M の著作権保護技術である C P P M (Content Protection for Pre-Recorded Media)、並びに記録型 D V D 、メモリカードに関する著作権保護技術 C R P M (Content Protection for Recordable Media) が提案されている。これらの方式は、コンテンツの暗号化や管理情報の格納等に問題が生じたときに、システムを更新でき、また、データをまるごとコピーしても再生を制限できる特徴を有している。D V D に関する著作権保護の方法に関しては、下記の非特許文献 1 に説明され、C R P M は、ライセンス管理者である米 4 C Entity, LLC が配布する下記の資料（非特許文献 2）に説明されている。

【 0 0 0 6 】

【非特許文献 1】

山田, 「D V D を起点に著作権保護空間を広げる」, 日経エレクトロニクス 200 1.8.13, p.143-153

【 0 0 0 7 】

【非特許文献 2】

"Content Protection for Recordable Media Specification DVD Book"、インターネット < U R L : <http://www.4Centity.com/> >

【 0 0 0 8 】

【発明が解決しようとする課題】

パーソナルコンピュータ（以下、適宜 P C と略す）環境下では、P C とドライブとが標準的インターフェースで接続されるために、標準的インターフェースの部分で秘密保持が必要なデータが知られたり、データが改ざんされるおそれがある。また、アプリケーションソフトウェアがリバースエンジニアリングされ、秘密情報が盗まれたり、改ざんされる危険がある。このような危険性は、記録再生装置が一体に構成された電子機器の場合では、生じることが少ない。

【0009】

著作権保護技術をPC上で実行されるアプリケーションプログラムへ実装する際には、その著作権保護技術の解析を防ぐため耐タンパー性を持たせるのが一般的である。しかしながら、耐タンパー性の強度を示す指標がなく、その結果、どの程度のリバースエンジニアリングへの対応を行うかは、インプレメンターの個々の判断や能力に委ねられているのが現状である。CSSの場合は、結果として破られてしまった。さらに、CSSの後に提案されたCPPMおよび記録型DVDに関する著作権保護技術CRPMにおいても、PCでのソフトウェア実装に関する問題解決に至る技術的方法の提案がなされていない。

【0010】

したがって、この発明の目的は、PC環境下でも著作権保護技術の安全性を確保することができ、また、正規のライセンスを受けないドライブの作成を防止し、さらに、確実にリボケーションを行うことが可能な記録再生装置、データ処理装置および記録再生処理システムを提供することにある。

【0011】

【課題を解決するための手段】

上述した課題を解決するために、請求項1の発明は、記録媒体固有の第1の情報を保持している記録媒体への暗号化されたデータを記録する記録部および記録媒体に記録されている暗号化されたデータを再生する再生部の少なくとも一方と、

正当な電子機器またはアプリケーションソフトウェアにのみ与えられる当該電子機器またはアプリケーションソフトウェア固有の第2の情報が格納される格納部と、

記録媒体固有の第1の情報と格納部に格納された第2の情報とに基づいて生成された鍵を用いて、データの暗号化および暗号化されたデータの復号の少なくとも一方を行うデータ処理装置と相互認証を行う接続部とを有することを特徴とする記録再生装置である。

【0012】

請求項3の発明は、少なくとも格納部に格納された第2の情報と記録媒体固有

の第1の情報とを用いて、当該格納された第2の情報が正当な電子機器またはアプリケーションソフトウェア固有の情報でない場合にリボケーションを行うリボーク処理部を有するデータ処理装置に対して、接続部が格納部に格納された第2の情報を送ることを特徴とする記録再生装置である。

【0013】

請求項5の発明は、格納部に格納された第2の情報と記録媒体固有の第1の情報とを用いて、当該格納された第2の情報が正当な電子機器またはアプリケーションソフトウェア固有の情報でない場合にリボケーションを行うリボーク処理部を有することを特徴とする記録再生装置である。

【0014】

請求項6の発明は、記録媒体固有の第1の情報を保持している記録媒体への暗号化されたデータを記録する記録部および記録媒体に記録されている暗号化されたデータを再生する再生部の少なくとも一方と、

正当な電子機器またはアプリケーションソフトウェア固有にのみ与えられる当該電子機器またはアプリケーションソフトウェア固有の第2の情報が格納される格納部と、

記録媒体固有の第1の情報と格納部に格納された第2の情報とに基づいて生成された鍵を用いて、データの暗号化および暗号化されたデータの復号の少なくとも一方を行うデータ処理装置と相互認証を行う接続部と

少なくとも接続部を介してデータ処理装置から送られ、格納部に格納された第2の情報と、記録媒体固有の第1の情報とを用いて、当該格納された第2の情報が正当なアプリケーションソフトウェア固有の情報でない場合にリボケーションを行うリボーク処理部を有することを特徴とする記録再生装置である。

【0015】

請求項8の発明は、正当な電子機器またはアプリケーションソフトウェアにのみ与えられる当該電子機器またはアプリケーションソフトウェア固有の第2の情報を有するとともに、記録媒体固有の第1の情報を保持している記録媒体への暗号化されたデータの記録および記録媒体に記録されている暗号化されたデータの再生の少なくとも一方を行う記録再生装置と相互認証を行う接続部と、

接続部を介して記録再生装置から送られた、記録媒体固有の第1の情報と電子機器またはアプリケーションソフトウェア固有の第2の情報とに基づいて生成された鍵を用いて、データの暗号化および暗号化されたデータの復号の少なくとも一方を行う処理部と

を有することを特徴とするデータ処理装置である。

【0016】

請求項10の発明は、接続部を介して記録再生装置から送られた第2の情報と、記録媒体固有の第1の情報とを用いて、第2の情報が正当な電子機器またはアプリケーションソフトウェア固有の情報でない場合にリボケーションを行うリボーク処理部を有することを特徴とするデータ処理装置である。

【0017】

請求項12の発明は、少なくとも記録再生装置に格納された第2の情報と、記録媒体固有の第1の情報とを用いて、当該格納された第2の情報が正当な電子機器またはアプリケーションソフトウェア固有の情報でない場合にリボケーションを行うリボーク処理部を有する記録再生装置と接続することを特徴とするデータ処理装置である。

【0018】

請求項13の発明は、正当なアプリケーションソフトウェアにのみ与えられるアプリケーションソフトウェア固有の第2の情報を有する格納部と、

記録媒体固有の第1の情報を保持している記録媒体への暗号化されたデータの記録および記録媒体に記録されている暗号化されたデータの再生の少なくとも一方を行う記録再生装置と相互認証を行う接続部と、

記録媒体固有の第1の情報と格納部に格納された第2の情報とに基づいて生成された鍵を用いて、データの暗号化および暗号化されたデータの復号の少なくとも一方を行う処理部とを有し、

格納部に格納された第2の情報が正当なアプリケーションソフトウェア固有の情報でない場合にリボケーションを行うリボーク処理部を有する記録再生装置に対して、格納部に格納された第2の情報を送ることを特徴とするデータ処理装置である。

【0019】

請求項15の発明は、記録媒体固有の第1の情報を保持している記録媒体への暗号化されたデータの記録および記録媒体に記録されている暗号化されたデータの再生の少なくとも一方が可能であると共に、正当な電子機器またはアプリケーションソフトウェア固有にのみ与えられる電子機器またはアプリケーションソフトウェア固有の第2の情報を有する記録再生装置と、

少なくとも格納された第2の情報と、記録媒体固有の第1の情報とに基づいて生成された鍵を用いて、データの暗号化および暗号化されたデータの復号の少なくとも一方を行うデータ処理装置と

を有することを特徴とする記録再生処理システムである。

【0020】

請求項16の発明は、データ処理装置が記録媒体固有の第1の情報と格納された第2の情報を用いて、当該格納された第2の情報が正当な電子機器またはアプリケーションソフトウェア固有の情報でない場合にリボケーションを行うリポート処理部を有することを特徴とする記録再生処理システムである。

【0021】

請求項17の発明は、記録再生装置が記録媒体固有の第1の情報と格納された第2の情報を用いて、当該格納された第2の情報が正当な電子機器またはアプリケーションソフトウェア固有の情報でない場合にリボケーションを行うリポート処理部を有することを特徴とする記録再生処理システムである。

【0022】

請求項18の発明は、正当な電子機器またはアプリケーションソフトウェアにのみ与えられる当該電子機器またはアプリケーションソフトウェア固有の情報として格納された第2の情報を有するとともに、記録媒体固有の第1の情報を保持している記録媒体への暗号化されたデータの記録および記録媒体に記録されている暗号化されたデータの再生の少なくとも一方を行う記録再生装置と、

格納された第2の情報と、記録媒体固有の第1の情報とに基づいて生成された鍵を用いてデータの暗号化、または暗号化されたデータの復号が可能なデータ処理装置とからなり、

格納された第2の情報が正当なアプリケーションソフトウェア固有の情報でない場合にリボケーションを行うリボーク処理部を有する記録再生装置に対して、データ処理装置が格納部に格納された第2の情報を送ることを特徴とする記録再生処理システムである。

【0023】

この発明では、正当な電子機器またはアプリケーションソフトウェアにのみ与えられる電子機器またはアプリケーションソフトウェア固有の第2の情報例えばデバイスキーが記録再生装置に格納されている。したがって、デバイスキーを外部から読み取ることが不可能となり、データ処理装置にインストールされるアプリケーションは、著作権保護技術に関するデータを持つ必要がなくなる。それによって、ソフトウェアのリバースエンジニアリングによる解析に対する耐性を持つことができ、著作権保護技術の安全性を確保することができる。また、記録媒体を扱う正当な記録再生装置となるためには、デバイスキーのような著作権保護技術に関する秘密情報を必要とするので、正規のライセンスを受けずに正規品になりすますようなクローン装置の作成を防止できる効果がある。

【0024】

この発明では、著作権保護技術に関するアルゴリズムの一部例えばメディアユニークキーの演算が記録再生装置内に実装されている。その結果、データ処理装置にインストールされるアプリケーションは、著作権保護技術に関するアルゴリズムの一部しか持たないで良く、それによって、ソフトウェアのリバースエンジニアリングによる解析に対する耐性を持つことができ、著作権保護技術の安全性を確保することができる。

【0025】

【発明の実施の形態】

この発明の理解の容易のために、最初に図1を参照して著作権保護技術例えばDVD用CPRMのアーキテクチャについて説明する。図1において、参照符号1が例えばCPRM規格に準拠したDVD-R/RW、DVD-RAM等の記録型DVDメディアを示し、参照符号2が例えばCPRM規格に準拠したレコーダを示し、参照符号3が例えばCPRM規格に準拠したプレーヤを示す。レコーダ

2 およびプレーヤ 3 は、機器またはアプリケーションソフトウェアである。

【0026】

未記録ディスクの状態において、DVDメディア 1 の最内周側のリードインエリアのBCA (Burst Cutting Area) またはNBCA (Narrow Burst Cutting Area) と称されるエリアには、メディアID 11 が記録され、リードインエリアのエンボスまたはプリ記録データゾーンには、メディアキーブロック（以下、MKB と適宜略す）12 が予め記録されている。メディアID 11 は、個々のメディア単位例えばディスク 1 枚毎に異なる番号であり、メディアの製造者コードとシリアル番号から構成される。メディアID 11 は、メディアキーを個々のメディアで異なるメディアユニークキーへ変換する際に必要となる。メディアキーブロック MKB は、メディアキーの導出、並びに機器のリボケーション（無効化）を実現するための鍵束である。これらのメディアID およびメディアキーブロックは、記録媒体固有の第 1 の情報である。

【0027】

ディスク 1 の書き換えまたは追記可能なデータ領域には、コンテンツキーで暗号化された暗号化コンテンツ 13 が記録される。暗号化方式としては、C2 (Cryptomeria Cipherring) が使用される。

【0028】

DVDメディア 1 には、暗号化タイトルキー 14 およびCCI (Copy Control Information) 15 が記録される。暗号化タイトルキー 14 は、暗号化されたタイトルキー情報であり、タイトルキー情報は、タイトル毎に付加される鍵情報である。CCI は、コピーノーマ、コピーワンス、コピーフリー等のコピー制御情報である。

【0029】

レコーダ 2 は、デバイスキー 21、プロセスMKB 22、C2__G 23、乱数発生器 24、C2__E 25、C2__G 26 およびC2__ECBC 27 の構成要素を有する。プレーヤ 3 は、デバイスキー 31、プロセスMKB 32、C2__G 33、C2__D 35、C2__G 36 およびC2__DCBC 37 の構成要素を有する。

【0030】

デバイスキー 21、31は、個々の装置メーカ、またはアプリケーションソフトウェアベンダー毎に発行された識別番号である。デバイスキーは、ライセンス管理者によって正当な電子機器またはアプリケーションソフトウェアにのみ与えられる当該電子機器またはアプリケーションソフトウェア固有の情報である。DVDメディア1から再生されたMKB12とデバイスキー21とがプロセスMKB22において演算されることによって、リボケーションされたかどうかの判別ができる。レコーダ2におけるのと同様に、プレーヤ3においても、MKB12とデバイスキー31とがプロセスMKB32において演算され、リボケーションされたかどうかの判別がなされる。

【0031】

さらに、プロセスMKB22、32のそれぞれにおいて、MKB12とデバイスキー21、31からメディアキーが算出される。MKB12の中にレコーダ2またはプレーヤ3のデバイスキーが入っておらず、演算された結果が予め決められたある値例えばゼロの値と一致した場合、そのデバイスキーを持つレコーダ2またはプレーヤ3が正当なものでないと判断される。すなわち、そのようなレコーダ2またはプレーヤ3がリボケーションされる。

【0032】

C2__G23、33は、それぞれ、メディアキーとメディアIDとを演算し、メディアユニークキーを導出する処理である。

【0033】

乱数発生器(RNG:Random Number Generator)24は、タイトルキーの生成に利用される。乱数発生器24からのタイトルキーがC2__E25に入力され、タイトルキーがメディアユニークキーで暗号化される。暗号化タイトルキー14がDVDメディア1に記録される。

【0034】

プレーヤ3では、DVDメディア1から再生された暗号化タイトルキー14とメディアユニークキーとがC2__D35に供給され、暗号化タイトルキーがメディアユニークキーで復号化され、タイトルキーが得られる。

【0035】

レコーダ2においては、CCIとタイトルキーとがC2__G26に供給され、コンテンツキーが導出される。コンテンツキーがC2__ECBC27に供給され、コンテンツキーを鍵としてコンテンツが暗号化される。暗号化コンテンツ13がDVDメディア1に記録される。

【0036】

プレーヤ3においては、CCIとタイトルキーとがC2__G36に供給され、コンテンツキーが導出される。コンテンツキーがC2__ECBC37に供給され、DVDメディア1から再生された暗号化コンテンツ13がコンテンツキーを鍵として復号される。

【0037】

図1の構成において、レコーダ2による記録の手順について説明する。レコーダ2は、DVDメディア1からMKB12を読み出し、プロセスMKB22によってデバイスキー21とMKB12とを演算し、メディアキーを計算する。演算結果が予め定められた値を示すならば、デバイスキー21（レコーダ2の機器またはアプリケーション）がMKBによってリボークされたと判定され、レコーダ2は、以後の処理を中断し、DVDメディア1への記録を禁止する。若し、メディアキーの値が予め定められた値以外であれば、処理を継続する。

【0038】

次に、レコーダ2は、DVDメディア1からメディアID11を読み、メディアキーと共にメディアIDをC2__G23に入力しメディア毎に異なるメディアユニークキーが演算される。乱数発生器24で発生させたタイトルキーがC2__E25で暗号化され、暗号化タイトルキー14としてDVDメディア1に記録される。また、タイトルキーとコンテンツのCCI情報がC2__G26で演算され、コンテンツキーが導出される。コンテンツキーでコンテンツをC2__ECBC27で暗号化し、DVDメディア1上に暗号化コンテンツ13としてCCI15と共に記録する。

【0039】

プレーヤ3による再生の手順について説明する。最初にMKB12をDVDメ

ディア1から読み出し、デバイスキー31とMKB12を演算し、リボケーションの確認がなされる。デバイスキー31、すなわち、プレーヤ3の機器またはアプリケーションがリボークされない場合には、メディアIDを使用してメディアユニークキーが演算され、読み出された暗号化タイトルキー14とメディアユニークキーからタイトルキーが演算される。タイトルキーとCCI15とがC2__G36に入力され、コンテンツキーが導出される。コンテンツキーがC2__DCBC37に入力され、コンテンツキーを鍵として、DVDメディア1から再生された暗号化コンテンツ13に対してC2__DCBC37の演算が施される。その結果、暗号化コンテンツ13が復号される。

【0040】

このように、コンテンツの復号に必要なコンテンツキーを得るためには、DVDメディアの1枚毎に異なるメディアIDが必要となるので、たとえメディア上の暗号化コンテンツが忠実に他のメディアにコピーされても、他のメディアのメディアIDがオリジナルのメディアIDと異なるために、コピーされたコンテンツを復号することができず、コンテンツの著作権を保護することができる。

【0041】

上述した図1の構成は、記録再生機器として構成されたものである。この発明は、DVDメディア1に対するコンテンツ保護処理をPC環境下で扱う場合に適用される。図2を参照して現行の方式によるPCとドライブの役割分担を示す。図2において、参照符号4が上述したCPRM規格に準拠したDVDメディア1を記録および再生する記録再生装置としてのDVDドライブを示す。

【0042】

参照符号5がデータ処理装置としてのホスト例えばPCを示す。ホスト5は、DVDメディア1に記録可能で、DVDメディア1から再生可能なコンテンツを扱うことができ、且つDVDドライブ4と接続されてデータ交換が可能な装置またはアプリケーションソフトウェアである。例えばPCに対してアプリケーションソフトウェアがインストールされることによってホスト5が構成される。

【0043】

DVDドライブ4とホスト5との間がインターフェース4aで接続されている

。インターフェース 4 a は、A T A P I (AT Attachment with Packet Interface), S C S I (Small Computer System Interface), U S B (Universal Serial Bus), I E E E (Institute of Electrical and Electronics Engineers) 1 3 9 4 等である。

【 0 0 4 4 】

D V D メディア 1 には、メディア I D 1 1、メディアキープブロック 1 2 および A C C (Authentication Control Code) が予め記録されている。A C C は、D V D ドライブ 4 とホスト 5 との間の認証が D V D メディア 1 によって異なるようにするために予め D V D メディア 1 に記録されたデータである。

【 0 0 4 5 】

D V D ドライブ 4 は、A C C 1 6 を D V D メディア 1 から読み出す。D V D メディア 1 から読み出された A C C 1 6 が D V D ドライブ 4 の A K E (Authentication and Key Exchange) 4 1 に入力されると共に、ホスト 5 へ転送される。ホスト 5 は、受け取った A C C を A K E 5 1 に入力する。A K E 4 1 および 5 1 は、乱数データを交換し、この交換した乱数と A C C の値とから認証動作の度に異なる値となる共通のセッションキー（バスキーと称する）を生成する。

【 0 0 4 6 】

バスキーが M A C (Message Authentication Code) 演算ブロック 4 2 および 5 2 にそれぞれ供給される。M A C 演算ブロック 4 2 および 5 2 は、A K E 4 1 および 5 1 でそれぞれ得られたバスキーをパラメータとして、メディア I D およびメディアキープブロック 1 2 の M A C を計算するプロセスである。M K B とメディア I D の完全性 (integrity) をホスト 5 が確認するために利用される。

【 0 0 4 7 】

M A C 4 2 および 5 2 によってそれぞれ計算された M A C がホスト 5 の比較 5 3 において比較され、両者の値が一致するかどうか判定される。これらの M A C の値が一致すれば、M K B とメディア I D の完全性が確認されたことになる。比較出力でスイッチ S W 1 が制御される。

【 0 0 4 8 】

スイッチ S W 1 は、D V D ドライブ 4 の D V D メディア 1 の記録または再生経

路と、ホスト 5 の暗号化／（または）復号モジュール 5 4 との間の信号路を ON／OFF するものとして示されている。なお、スイッチ SW 1 は、信号路の ON／OFF を行うものとして示されているが、より実際には、ON の場合にホスト 5 の処理が継続し、OFF の場合にホスト 5 の処理が停止することを表している。暗号化／復号モジュール 5 4 は、メディアユニークキーと暗号化タイトルキーと CCI とからコンテンツキーを算出し、コンテンツキーを鍵としてコンテンツを暗号化コンテンツ 1 3 へ暗号化し、またはコンテンツキーを鍵として暗号化コンテンツ 1 3 を復号する演算ブロックである。

【0049】

メディアユニークキー演算ブロック 5 5 は、MKB 1 2 とメディア ID とデバイスキー 5 6 とからメディアユニークキーを演算する演算ブロックである。すなわち、図 1 に示すレコードまたはプレーヤと同様に、デバイスキーと MKB 1 2 とからメディアキーが演算され、さらに、メディアキーとメディア ID 1 1 とからメディアユニークキーが演算される。メディアキーが所定の値となった場合には、その電子機器またはアプリケーションソフトウェアが正当なものではないと判断され、リボークされる。したがって、メディアユニークキー演算ブロック 5 5 は、リボケーションを行うリボーク処理部としての機能も有する。

【0050】

記録時に、比較 5 3 によって完全性が確認された場合には、スイッチ SW 1 が ON され、暗号化／復号モジュール 5 4 からスイッチ SW 1 を通じてドライブ 4 に対して、暗号化コンテンツ 1 3、暗号化タイトルキー 1 4 および CCI 1 5 が供給され、DVD メディア 1 に対してそれぞれ記録される。再生時に、比較 5 3 によって完全性が確認された場合には、スイッチ SW 1 が ON され、DVD メディア 1 からそれぞれ再生された暗号化コンテンツ 1 3、暗号化タイトルキー 1 4 および CCI 1 5 がスイッチ SW 1 を通じてホスト 5 の暗号化／復号モジュール 5 4 に対して供給され、暗号化コンテンツが復号される。

【0051】

図 3 は、図 2 に示す現行の PC 環境下の DVD メディアを利用するシステムにおいて、DVD メディア 1 と、DVD ドライブ 4 と、ホスト 5 との間の信号の授

受の手順を示す。ホスト5がDVDドライブ4に対してコマンドを送り、DVDドライブ4がコマンドに応答した動作を行う。

【0052】

最初に、ホスト5からの要求に応じてDVDメディア1上のACCがシークされ、読み出される（ステップS1）。次のステップS2において、読み出されたACCがAKE41に入力されると共に、ホスト5へ転送され、ホスト5では、受け取ったACCがAKE51へ入力される。AKE41および51は、乱数データを交換し、この交換した乱数とACC16の値から認証動作の度に異なる値となるセッションキーとしてのバスキーを生成し、バスキーをDVDドライブ4とホスト5が共有する。相互認証が成立しなかった場合では、処理が中断する。

【0053】

認証動作は、電源のONまたはOFF時並びにディスクの交換時には、必ず行われる。また、記録ボタンを押して記録動作を行う場合、並びに再生ボタンを押して再生動作を行う場合に、認証動作を行うようにしても良い。一例として、記録ボタンまたは再生ボタンを押した時に、認証がなされる。

【0054】

認証が成功すると、次に、ステップS3において、ホスト5がDVDドライブ4に対して、DVDメディア1からのMKB（メディアキーブロック）パック#0の読み出しを要求する。MKBは、パック0～パック15の16セクタが12回繰り返してリードインエリアに記録されている。パック単位で、エラー訂正符号化がなされている。

【0055】

DVDドライブ4がステップS4においてMKBのパック#0を読みに行き、ステップS5において、パック#0が読み出される。DVDドライブ4は、モディファイドMKBをホスト5へ戻す（ステップS6）。すなわち、MKBを読み出す際に、バスキーをパラメータとしてMAC値を計算し、MKBに対してMAC値を付加してホスト5へデータを転送する。パック#0以外の残りのMKBパックの要求と、DVDドライブ4の読み出し動作と、モディファイドMKBパックの転送動作とがMKBのパックがなくなるまで、例えばパック#15が読み出

され、ホスト5へ転送されるまで、ステップS7およびS8によって繰り返される。

【0056】

次に、ホスト5がDVDドライブ4に対してメディアIDを要求する。DVDドライブ4がDVDメディア1に記録されているメディアIDを読みに行き、ステップS11において、メディアIDが読み出される。DVDドライブ4は、メディアIDを読み出す際に、バスキーをパラメータとしてそのMAC値を計算し、ステップS12において、読み出されたメディアIDに対してMAC値m1を付加してホスト5へデータを転送する。

【0057】

ホスト5では、DVDドライブ4から受け取ったMKB12およびメディアID11からバスキーをパラメータとして再度MAC値を計算し、計算したMAC値とDVDドライブ4から受け取ったMAC値とを比較53で比較し、両者が一致したならば、正しいMKBおよびメディアIDを受け取ったと判定して、スイッチSW1をONに設定して処理を先に進める。逆に両者が一致しなかったならば、MKBおよびメディアIDが改ざんされたものと判定して、スイッチSW1をOFFに設定して処理を中断する。

【0058】

ステップS13において、ホスト5がDVDドライブ4に対して暗号化コンテンツを要求し、ステップS14において、DVDドライブ4が暗号化コンテンツを読み出し、ステップS13において、読み出した暗号化コンテンツがホスト5に転送される。ホスト5のメディアユニークキー演算ブロック55では、デバイスキー56とMKB12とメディアID11とによってメディアユニークキーが計算される。そして、メディアユニークキーが暗号化／復号モジュール54に供給され、暗号化タイトルキー14、CCI15からコンテンツキーが求められ、コンテンツキーを鍵としてDVDメディア1から読み出された暗号化コンテンツが復号され、また、DVDメディア1に対して記録されるコンテンツが暗号化される。

【0059】

図4のフローチャートにおいて、ステップST1は、MAC演算ブロック42でバスキーをパラメータとして求められたMAC計算値と、MAC演算ブロック53でバスキーをパラメータとして求められたMAC計算値とを比較するステップである。両者が一致すれば、スイッチSW1がステップST2においてONとされ、両者が一致しない場合では、スイッチSW1がステップST3においてOFFとされ、処理が停止する。

【0060】

図2に示すようなPC環境下のシステムに対して適用されるこの発明の第1の実施形態を図5に示す。第1の実施形態は、ホスト5の側で秘密情報とされているデバイスキーをDVDドライブ4側に記憶するようにしたものである。デバイスキーは、上述したように、リボケーション動作とメディアキーの導出に使用される情報である。

【0061】

図5において、参照符号46がDVDドライブ4側に記憶されたデバイスキーである。デバイスキー46をセキュアにホスト5に伝送するために、デバイスキー46が暗号化例えばDES(Data Encryption Standard)エンクリプタ47に入力され、バスキーで暗号化される。暗号化デバイスキーがドライブホストインターフェース4aを通じてホスト5へ転送される。

【0062】

比較53においてMAC値が一致すると検出された場合、すなわち、完全性が確認できた場合にのみONするスイッチSW2を介して暗号化デバイスキーがDESデクリプタ57に入力される。なお、スイッチSW2は、信号路のON/OFFを行うものとして示されているが、より実際には、スイッチSW1と同様に、ONの場合にホスト5の処理が継続し、OFFの場合にホスト5の処理が停止することを表している。DESデクリプタ57には、バスキーが供給され、デバイスキーが復号される。

【0063】

復号されたデバイスキーがメディアユニークキー演算ブロック55に供給され、MKB12とメディアIDとデバイスキー46とからメディアユニークキーが

演算される。すなわち、MKB 12とデバイスキー46とを使用してメディアキーが計算され、メディアIDとメディアキーとを使用してメディアユニークキーが計算される。メディアユニークキー演算ブロック55において、計算されたメディアキーが所定の値となる場合には、デバイスキー、すなわち、DVDドライブ4がリボークされ、処理が停止される。メディアユニークキー演算ブロック55は、リボーク処理部の機能を有している。

【0064】

そして、メディアユニークキーが暗号化／復号モジュール54に供給され、暗号化タイトルキー14、CCI 15からコンテンツキーが求められ、コンテンツキーを使用してDVDメディア1から読み出された暗号化コンテンツが復号され、また、DVDメディア1に対して記録されるコンテンツが暗号化される。

【0065】

図6は、第1の実施形態の処理の手順を示す。ACCのシークおよびリード（ステップS21）からメディアIDとm1をリターン（ステップS32）までの処理は、図3に示すものと同様であるので、この処理については、簡単に説明する。ステップS21では、ACCがシークされ、読み出され、ステップS22において認証が成功すると、認証動作の度に異なる値となるセッションキーとしてのバスキーが生成される。

【0066】

次に、ステップS23において、ホスト5がMKB（メディアキーブロック）パック#0の読み出しをDVDドライブ4に要求し、DVDドライブ4がステップS24においてMKBパック#0を読みに行き、ステップS25において、パック#0が読み出される。ステップS26で、DVDドライブ4は、MKBを読み出す際に、バスキーをパラメータとしてMAC値を計算し、MKBに対してMAC値を付加したデータ（モディファイドMKB）をホスト5へ戻す。ステップS27およびS28において、パック#0以外の残りのMKBパックの要求と、読み出し動作と、転送動作とがなされる。

【0067】

次に、ホスト5がメディアIDを要求し（ステップS29）、DVDドライブ

4 がメディア ID を読みに行き (ステップ S 3 0)、ステップ S 3 1 において、メディア ID が読み出される。DVD ドライブ 4 は、メディア ID を読み出す際に、バスキーをパラメータとしてその MAC 値を計算し、ステップ S 3 2 において、読み出されたメディア ID に対して MAC 値 m 1 を付加してホスト 5 ヘデータを転送する。

【0068】

ホスト 5 では、DVD ドライブ 4 から受け取った MKB 1 2 およびメディア ID 1 1 からバスキーをパラメータとして再度 MAC 値を計算する。計算した MAC 値と DVD ドライブ 4 から受け取った MAC 値とが一致したならば、正しい MKB およびメディア ID を受け取ったと判定して、スイッチ SW 1 を ON に設定して処理を先に進める。逆に両者が一致しなかったならば、MKB およびメディア ID が改ざんされたものと判定して、スイッチ SW 1 を OFF に設定して処理を停止する。

【0069】

ステップ S 3 3 において、ホスト 5 が DVD ドライブ 4 に対してデバイスキーを要求する。DVD ドライブ 4 は、デバイスキー 4 6 を DES エンクリプタ 4 7 によって暗号化し、暗号化デバイスキーをホスト 5 に送る (ステップ S 3 4)。ホスト 5 は、バスキーを使用して DES デクリプタ 5 7 によってデバイスキーを復号する。

【0070】

ステップ S 3 5 において、ホスト 5 が DVD ドライブ 4 に対して暗号化コンテンツを要求し、ステップ S 3 6 において、DVD ドライブ 4 が暗号化コンテンツを読み出し、ステップ S 3 5 において、読み出した暗号化コンテンツがホスト 5 に転送される。ホスト 5 のメディアユニークキー演算ブロック 5 5 では、デバイスキー 4 6 と MKB 1 2 とメディア ID 1 1 とによってメディアユニークキーが計算される。そして、メディアユニークキーが暗号化／復号モジュール 5 4 に供給され、暗号化コンテンツが復号され、また、DVD メディア 1 に対して記録されるコンテンツが暗号化される。

【0071】

上述した第1の実施形態では、著作権保護技術に関する秘密情報であるデバイスキーがDVDドライブ4内に実装されている。例えばフラッシュメモリ等のLSI (Large Scale Integrated Circuit: 大規模集積回路) 内にデバイスキーが実装される。LSI内のデバイスキーを外部から読み取ることが不可能とされている。ホスト5にインストールされるアプリケーションソフトウェアは、著作権保護技術に関する秘密情報を持つ必要がなくなる。それによって、ソフトウェアのリバースエンジニアリングによる解析に対する耐性を持つことができ、著作権保護技術の安全性を確保することができる。

【0072】

また、DVDメディア1を扱う正当なドライブとなるためには、デバイスキーのような著作権保護技術に関する秘密情報を必要とするので、正規のライセンスを受けずに正規品になりすますようなクローン・ドライブの作成を防止できる効果がある。

【0073】

PC環境下で実施されるこの発明の第2の実施形態を図7に示す。第2の実施形態は、ホスト5の側で秘密情報とされているデバイスキーを二つの要素に分解し、その内の一方の要素をDVDドライブ4側に記憶するようにしたものである。

【0074】

図7において、参照符号46aがDVDドライブ4側に記憶されたデバイスキーの前半部である。デバイスキーの前半部とは、デバイスキーの後半部と組み合わせることによって完全なデバイスキーを構成するデバイスキーの一部分のことである。デバイスキーの前半部46aが暗号化例えばDESエンクリプタ47に入力され、バスキーで暗号化される。暗号化デバイスキーの前半部がドライブホストインターフェース4aを通じてホスト5へ転送される。

【0075】

比較53においてMAC値が一致すると検出された場合にのみONするスイッチSW2を介して暗号化デバイスキーの前半部がDESデクリプタ57に入力される。DESデクリプタ57には、バスキーが供給され、デバイスキーの前半部

がDESデクリプタ57によって復号される。

【0076】

参照符号56aがデバイスキーの後半部を示す。DESデクリプタ57によって復号されたデバイスキーの前半部46aとデバイスキーの後半部56aとがデバイスキー合成部58に入力され、両者が合成されることで、デバイスキーが得られる。

【0077】

得られたデバイスキーがメディアユニークキー演算ブロック55に供給され、MKB12とメディアIDとデバイスキー46とからメディアユニークキーが演算される。そして、メディアユニークキーが暗号化／復号モジュール54に供給される。暗号化タイトルキー14、CCI15からコンテンツキーが求められ、コンテンツキーを使用してDVDメディア1から読み出された暗号化コンテンツが復号され、また、DVDメディア1に対して記録されるコンテンツが暗号化される。

【0078】

上述した第2の実施形態は、デバイスキーを二つの要素に分解している点を除くと、第1の実施形態と同様のものであり、処理の手順は、図6と同様のものであり、その図示については省略する。

【0079】

第2の実施形態では、著作権保護技術に関するデータとしてデバイスキーの一部がドライブ4内に実装されている。例えばLSI内にデバイスキーの一部が実装される。その結果、ホスト5にインストールされるアプリケーションは、著作権保護技術に関するデータを一部しか持たないで良く、それによって、ソフトウェアのリバースエンジニアリングによる解析に対する耐性を持つことができ、著作権保護技術の安全性を確保することができる。

【0080】

また、DVDメディア1を扱う正当なドライブとなるためには、デバイスキーのような著作権保護技術に関する秘密情報を必要とするので、正規のライセンスを受けずに正規品になりすますようなクローン・ドライブの作成を防止できる効

果がある。さらに、デバイスキーの前半部 46 a とその後半部 56 a が共に正しい場合にのみ、電子機器またはアプリケーションソフトウェアが正当なものとされるので、DVDドライブ4およびホスト5の両方について、リボーク処理を行うことが可能となる。

【0081】

図8は、この発明の第3の実施形態を示す。第3の実施形態では、デバイスキー46をDVDドライブ4が持ち、さらに、参照符号48で示すメディアユニークキー演算ブロックをDVDドライブ4が持つようにしたものである。

【0082】

第3の実施形態では、メディアユニークキー演算ブロック48がDVDドライブ4に設けられているので、DVDメディア1から再生されたMKBおよびメディアIDをホスト5へ転送することが不要となる。その結果、MAC演算ブロック、計算されたMAC値の比較および比較出力で制御されるスイッチが不要となる。また、リボケーションもホスト5に依存することがなくなり、DVDメディア1とDVDドライブ4だけで処理が完結するようになる。

【0083】

DVDドライブ4に設けられたメディアユニークキー演算ブロック48において、MKB12とメディアIDとデバイスキー46とからメディアユニークキーが演算される。すなわち、MKB12とデバイスキー46とを使用してメディアキーが計算され、メディアID11とメディアキーとを使用してメディアユニークキーが計算される。メディアユニークキーをセキュアにホスト5に伝送するために、メディアユニークキーがDESエンクリプタ49に供給され、バスキーを使用して暗号化される。暗号化されたメディアユニークキーがホスト5のDESデクリプタ59に供給され、バスキーを使用して復号される。

【0084】

そして、復号されたメディアユニークキーが暗号化／復号モジュール54に供給され、暗号化タイトルキー14、CCI15からコンテンツキーが求められ、コンテンツキーを使用してDVDメディア1から読み出された暗号化コンテンツが復号され、また、DVDメディア1に対して記録されるコンテンツが暗号化さ

れる。

【0085】

図9は、第3の実施形態の処理の手順を示す。ACCのシークおよびリード（ステップS41）から残りのMKBパックのリード（ステップS48）までの処理は、図3に示すものと同様であるので、この処理については、簡単に説明する。

【0086】

ステップS42では、認証が行われ、認証が成功すると、認証動作の度に異なる値となるセッションキーとしてのバスキーが生成される。次に、ステップS43において、ホスト5がMKB（メディアキーブロック）パック#0の読み出しをDVDドライブ4に要求し、DVDドライブ4がステップS44においてMKBパック#0を読みに行き、ステップS45において、パック#0が読み出される。ステップS46で、DVDドライブ4は、MKBを読み出す際に、バスキーをパラメータとしてMAC値を計算し、MKBに対してMAC値を付加したデータをホスト5へ転送する。ステップS47およびS48において、パック#0以外の残りのMKBパックの要求と、読み出し動作と、転送動作とがなされる。

【0087】

次に、ステップS49において、ホスト5がメディアユニークキーを要求すると、DVDドライブ4が暗号化メディアユニークキーをホスト5に送る（ステップS50）。そして、メディアユニークキーが暗号化／復号モジュール54に供給される。ステップS51において、ホスト5が暗号化コンテンツを要求すると、DVDドライブ4が暗号化コンテンツをリードし（ステップS52）、暗号化／復号モジュール54によって暗号化コンテンツが復号され、また、DVDメディア1に対して記録されるコンテンツが暗号化される。

【0088】

図10は、この発明の第4の実施形態を示す。第4の実施形態では、第3の実施形態と同様に、メディアユニークキー演算ブロック48をDVDドライブ4が持ち、また、ホスト5がデバイスキー56を持ち、ホスト5からDVDドライブ4へデバイスキー56をセキュアに転送するものである。

【0089】

第4の実施形態では、メディアユニークキー演算ブロック48がDVDドライブ4に設けられているので、DVDメディア1から再生されたMKBおよびメディアIDをホスト5へ転送することが不要となる。その結果、MAC演算ブロック、計算されたMAC値の比較および比較出力で制御されるスイッチが不要となる。

【0090】

ホスト5のデバイスキー56がDESエンクリプタ59bに供給され、バスキーを鍵として暗号化される。暗号化デバイスキーがDVDドライブ4のDESデクリプタ49bに転送され、デバイスキーがDVDドライブ4において復号される。復号されたデバイスキーがメディアユニークキー演算ブロック48に入力される。

【0091】

DVDドライブ4に設けられたメディアユニークキー演算ブロック48において、MKB12とメディアIDとデバイスキー46とからメディアユニークキーが演算される。すなわち、MKB12とデバイスキー46とを使用してメディアキーが計算され、メディアID11とメディアキーとを使用してメディアユニークキーが計算される。メディアユニークキーがDESエンクリプタ49aに供給され、バスキーを使用して暗号化される。暗号化されたメディアユニークキーがホスト5のDESデクリプタ59aに供給され、バスキーを使用して復号される。

【0092】

そして、復号されたメディアユニークキーが暗号化／復号モジュール54に供給され、暗号化タイトルキー14、CCI15からコンテンツキーが求められ、コンテンツキーを使用してDVDメディア1から読み出された暗号化コンテンツが復号され、また、DVDメディア1に対して記録されるコンテンツが暗号化される。

【0093】

図11は、第4の実施形態の処理の手順を示す。ACCのシークおよびリード

(ステップS 6 1) から残りのMKBパックのリード(ステップS 6 8) までの処理は、図3に示すものと同様であるので、この処理については、簡単に説明する。

【0094】

ステップS 6 2では、認証が行われ、認証が成功すると、認証動作の度に異なる値となるセッションキーとしてのバスキーが生成される。次に、ステップS 6 3において、ホスト5がMKB(メディアキーブロック)パック# 0の読み出しをDVDドライブ4に要求し、DVDドライブ4がステップS 6 4においてMKBパック# 0を読みに行き、ステップS 6 5において、パック# 0が読み出される。ステップS 6 6で、DVDドライブ4は、MKBを読み出す際に、バスキーをパラメータとしてMAC値を計算し、MKBに対してMAC値を付加したデータをホスト5へ転送する。ステップS 6 7およびS 6 8において、パック# 0以外の残りのMKBパックの要求と、読み出し動作と、転送動作とがなされる。

【0095】

次に、ステップS 6 9において、暗号化デバイスキーをホスト5がDVDドライブ4に送る。DVDドライブ4において、メディアユニークキーが演算される。ステップS 7 0において、ホスト5がメディアユニークキーを要求すると、DVDドライブ4が暗号化メディアユニークキーをホスト5に送る(ステップS 7 1)。そして、メディアユニークキーが暗号化/復号モジュール5 4に供給される。ステップS 7 2において、ホスト5が暗号化コンテンツを要求すると、DVDドライブ4が暗号化コンテンツをリードし(ステップS 7 3)、暗号化/復号モジュール5 4によって暗号化コンテンツが復号され、また、DVDメディア1に対して記録されるコンテンツが暗号化される。

【0096】

上述した第3および第4の実施形態では、著作権保護技術に関するアルゴリズムの一部例えばメディアユニークキーの演算がドライブ4内に実装されている。例えばLSI内にメディアユニークキー演算ブロック4 8が実装される。その結果、ホスト5にインストールされるアプリケーションは、著作権保護技術に関するアルゴリズムの一部しか持たないで良く、それによって、ソフトウェアのリバ

ースエンジニアリングによる解析に対する耐性を持つことができ、著作権保護技術の安全性を確保することができる。

【0097】

また、第3の実施形態では、DVDメディア1を扱う正当なドライブとなるために、デバイスキーのような著作権保護技術に関する秘密情報を必要とするので、正規のライセンスを受けずに正規品になりすますようなクローン・ドライブの作成を防止できる効果がある。

【0098】

図12は、この発明の第5の実施形態を示す。上述した第1～第4の実施形態では、DVDの著作権保護技術であるCPRMに対してこの発明を適用したものである。一方、第5の実施形態は、図2に示す実際に運用されているCPRMのアーキテクチャを拡張した構成を有する。

【0099】

すなわち、ホスト5のメディアユニークキー演算ブロック61に対して、パラメータA62が関与し、また、暗号化／復号モジュール63に対して、パラメータB64が関与するようにしたものである。パラメータA62およびパラメータB64は、固定値およびDVDメディア1から読み出されたデータの何れであっても良い。

【0100】

現行のCPRMでは、MKBとデバイスキーからメディアキーを計算し、メディアキーとメディアIDからメディアユニークキーを計算している。CPRMを拡張したシステムにおいては、この計算の過程で、さらに、パラメータA62が関与し、暗号化／復号モジュール63では、コンテンツキーを計算する時に、さらにパラメータB64が関与する。第5の実施形態の処理の手順は、現行のCPRMと同様のものであり、その図示については省略する。

【0101】

図13は、この発明の第6の実施形態を示す。第6の実施形態は、実際に運用されているCPRMのアーキテクチャを拡張した構成を有し、デバイスキー46と、パラメータA62と、パラメータB64とをDVDドライブ4が持つように

したものである。これらのデバイスキー 46、パラメータ A 62 およびパラメータ B 64 をセキュアにホスト 5 に伝送するために、DES エンクリプタ 65 でこれらの情報がバスキーで暗号化される。

【0102】

比較 53 において MAC 値が一致すると検出された場合、すなわち、完全性が確認できた場合にのみ ON するスイッチ SW3 を介して暗号化されたデータが DES デクリプタ 66 に入力される。DES デクリプタ 66 には、バスキーが供給され、デバイスキー、パラメータ A 62 およびパラメータ B 64 が復号される。復号されたデバイスキーおよびパラメータ A がメディアユニークキー演算ブロック 61 に供給され、MKB 12 とメディア ID とデバイスキー 46 とパラメータ A とからメディアユニークキーが演算される。

【0103】

そして、メディアユニークキーおよびパラメータ B が暗号化／復号モジュール 63 に供給され、これらのデータを使用してコンテンツキーが求められ、コンテンツキーを使用してコンテンツの暗号化／復号がなされる。

【0104】

図 14 は、第 6 の実施形態の処理の手順を示す。ACC のシークおよびリード（ステップ S81）からメディア ID と m1 をリターン（ステップ S92）までの処理は、現行の CPRM の処理と同様であるので、この処理については、簡単に説明する。ステップ S81 では、ACC がシークされ、読み出され、ステップ S82 において認証が成功すると、認証動作の度に異なる値となるセッションキーとしてのバスキーが生成される。

【0105】

次に、ステップ S83 において、ホスト 5 が MKB（メディアキーブロック）パック #0 の読み出しを DVD ドライブ 4 に要求し、DVD ドライブ 4 がステップ S84 において MKB パック #0 を読みに行き、ステップ S85 において、パック #0 が読み出される。ステップ S86 で、DVD ドライブ 4 は、MKB を読み出す際に、バスキーをパラメータとして MAC 値を計算し、MKB に対して MAC 値を付加したデータ（モディファイド MKB）をホスト 5 へ戻す。ステップ

S 8 7 および S 8 8 において、パック # 0 以外の残りの MKB パックの要求と、読み出し動作と、転送動作とがなされる。

【0106】

次に、ホスト 5 がメディア ID を要求し（ステップ S 8 9）、DVD ドライブ 4 がメディア ID を読みに行き（ステップ S 9 0）、ステップ S 9 1 において、メディア ID が読み出される。DVD ドライブ 4 は、メディア ID を読み出す際に、バスキーをパラメータとしてその MAC 値を計算し、ステップ S 9 2 において、読み出されたメディア ID に対して MAC 値 m 1 を付加してホスト 5 へデータを転送する。

【0107】

ホスト 5 では、DVD ドライブ 4 から受け取った MKB 1 2 およびメディア ID 1 1 からバスキーをパラメータとして再度 MAC 値を計算する。計算した MAC 値と DVD ドライブ 4 から受け取った MAC 値とが一致したならば、正しい MKB およびメディア ID を受け取ったと判定して、スイッチ SW 1 およびスイッチ SW 3 を ON に設定して処理を先に進める。逆に両者が一致しなかったならば、MKB およびメディア ID が改ざんされたものと判定して、スイッチ SW 1 およびスイッチ SW 3 を OFF に設定して処理を停止する。

【0108】

ステップ S 9 3 において、ホスト 5 が DVD ドライブ 4 に対してデバイスキーとパラメータ A とパラメータ B とを要求する。DVD ドライブ 4 は、デバイスキー 4 6 とパラメータ A とパラメータ B とを DES エンクリプタ 6 5 によって暗号化し、暗号化データをホスト 5 に送る（ステップ S 9 4）。ホスト 5 は、バスキーを使用して DES デクリプタ 6 6 によってデバイスキーを復号する。

【0109】

ステップ S 9 5 において、ホスト 5 が DVD ドライブ 4 に対して暗号化コンテンツを要求し、ステップ S 9 6 において、DVD ドライブ 4 が暗号化コンテンツを読み出し、ステップ S 9 5 において、読み出した暗号化コンテンツがホスト 5 に転送される。ホスト 5 のメディアユニークキー演算ブロック 6 1 では、デバイスキー 4 6 と MKB 1 2 とメディア ID 1 1 とパラメータ A とによってメディア

ユニークキーが計算される。そして、メディアユニークキーが暗号化／復号モジュール 63 に供給され、暗号化コンテンツが復号され、また、DVDメディア 1 に対して記録されるコンテンツが暗号化される。

【0110】

図 15 は、この発明の第 7 の実施形態を示す。第 7 の実施形態では、メディアユニークキー演算ブロック 67 を DVD ドライブ 4 が持ち、また、ホスト 5 がデバイスキー 56 とパラメータ A 62 とパラメータ B 64 とを持ち、ホスト 5 から DVD ドライブ 4 へデバイスキー 56 およびパラメータ A 62 をセキュアに転送するものである。

【0111】

第 7 の実施形態では、メディアユニークキー演算ブロック 67 が DVD ドライブ 4 に設けられているので、DVD メディア 1 から再生された MKB およびメディア ID をホスト 5 へ転送することが不要となる。その結果、MAC 演算ブロック、計算された MAC 値の比較および比較出力で制御されるスイッチが不要となる。

【0112】

ホスト 5 のデバイスキー 56 およびパラメータ A 62 が DES エンクリプタ 68 に供給され、バスキーを鍵として暗号化される。暗号化データが DVD ドライブ 4 の DES デクリプタ 69 に転送され、デバイスキーおよびパラメータ A が DVD ドライブ 4 において復号される。復号されたデバイスキーおよびパラメータ A がメディアユニークキー演算ブロック 67 に入力される。

【0113】

DVD ドライブ 4 に設けられたメディアユニークキー演算ブロック 67 において、MKB 12 とメディア ID とデバイスキー 46 とパラメータ A とからメディアユニークキーが演算される。メディアユニークキーが DES エンクリプタ 70 に供給され、バスキーを使用して暗号化される。暗号化されたメディアユニークキーがホスト 5 の DES デクリプタ 71 に供給され、バスキーを使用して復号される。

【0114】

そして、復号されたメディアユニークキーが暗号化／復号モジュール 63 に供給され、暗号化タイトルキー 14、CCI 15 およびパラメータ A からコンテンツキーが求められ、コンテンツキーを使用して DVD メディア 1 から読み出された暗号化コンテンツが復号され、また、DVD メディア 1 に対して記録されるコンテンツが暗号化される。

【0115】

図 16 は、第 7 の実施形態の処理の手順を示す。ACC のシークおよびリード（ステップ S101）から残りの MKB パックのリード（ステップ S108）までの処理は、現行の CPRM の処理と同様であるので、この処理については、簡単に説明する。

【0116】

ステップ S102 では、認証が行われ、認証が成功すると、認証動作の度に異なる値となるセッションキーとしてのバスキーが生成される。次に、ステップ S103 において、ホスト 5 が MKB（メディアキーブロック）パック #0 の読み出しを DVD ドライブ 4 に要求し、DVD ドライブ 4 がステップ S104 において MKB パック #0 を読みに行き、ステップ S105 において、パック #0 が読み出される。ステップ S106 で、DVD ドライブ 4 は、MKB を読み出す際に、バスキーをパラメータとして MAC 値を計算し、MKB に対して MAC 値を付加したデータをホスト 5 へ転送する。ステップ S107 および S108 において、パック #0 以外の残りの MKB パックの要求と、読み出し動作と、転送動作とがなされる。

【0117】

次に、ステップ S109 において、暗号化デバイスキーおよび暗号化パラメータをホスト 5 が DVD ドライブ 4 に送る。次に、ステップ S110 において、ホスト 5 がメディアユニークキーを要求する。DVD ドライブ 4 において、メディアユニークキーが演算される。ステップ S111 において、DVD ドライブ 4 が暗号化メディアユニークキーをホスト 5 に送る。そして、メディアユニークキーが暗号化／復号モジュール 63 に供給される。ステップ S112 において、ホスト 5 が暗号化コンテンツを要求すると、DVD ドライブ 4 が暗号化コンテンツを

リードし（ステップ S 1 1 3）、暗号化／復号モジュール 6 3 によって暗号化コンテンツが復号され、また、DVDメディア 1 に対して記録されるコンテンツが暗号化される。

【0118】

この発明は、上述したこの発明の一実施形態等に限定されるものではなく、この発明の要旨を逸脱しない範囲内で様々な変形や応用が可能である。例えばデバイスキーを二つに分割し、ドライブおよびホストが各デバイスキーを持ち、また、メディアユニークキー演算ブロックをドライブが持つ構成も可能である。

【0119】

さらに、メディアユニークキーを演算するためのパラメータ A と、暗号化／復号のためのパラメータ B を使用する CPRM を拡張したシステムにおいては、パラメータ A, B がホスト側にある場合と、ドライブ側にある場合と、メディアに記録されており、ホストが読み出す場合との全てが可能である。また、パラメータ B を使用しないでも良い。パラメータ A, B をインターフェースを介して授受する場合には、暗号化がなされ、セキュアな伝送が必要とされる。

【0120】

また、上述した説明においては、著作権保護技術として CPRM および CPRM を拡張した例を挙げたが、CPRM 以外の著作権保護技術に対してもこの発明を適用することができる。また、PC ベースのシステムに対してこの発明が適用されるが、このことは、PC とドライブを組み合わせる構成にのみ限定されることを意味するものではない。例えば携帯型動画または静止画カメラの場合に、メディアとして光ディスクを使用し、メディアを駆動するドライブとドライブを制御するマイクロコンピュータが設けられる動画または静止画カメラシステムに対してもこの発明を適用することが可能である。

【0121】

【発明の効果】

この発明では、著作権保護技術に関する秘密情報である電子機器またはアプリケーションソフトウェア固有の情報例えばデバイスキーが記録再生装置内に実装されているので、DVD 処理装置にインストールされるアプリケーションソフト

ウェアは、著作権保護技術に関する秘密情報を持つ必要がなくなる。それによって、ソフトウェアのリバースエンジニアリングによる解析に対する耐性を持つことができ、著作権保護技術の安全性を確保することができる。

【0122】

また、電子機器またはアプリケーションソフトウェア固有の情報としてのデバイスキーを記録再生装置とデータ処理装置が分けて持つことによって、記録再生装置およびアプリケーションソフトウェアの両方について、リボーク処理を行うことが可能となる。

【0123】

さらに、この発明では、著作権保護技術に関するアルゴリズムの一部例えばメディアユニークキーの演算が記録再生装置内に実装されている。したがって、データ処理装置のアプリケーションソフトウェアは、著作権保護技術に関するアルゴリズムの一部しか持たないで良く、それによって、ソフトウェアのリバースエンジニアリングによる解析に対する耐性を持つことができ、著作権保護技術の安全性を確保することができる。

【図面の簡単な説明】

【図1】

先に提案されているレコーダ、プレーヤおよびDVDメディアからなるシステムを説明するためのブロック図である。

【図2】

PCベースのDVDメディア記録再生システムを説明するためのブロック図である。

【図3】

図2のシステムにおけるDVDドライブ4およびホスト5の処理の手順を説明するための略線図である。

【図4】

図2のシステムにおける認証動作を説明するためのフローチャートである。

【図5】

この発明の第1の実施形態によるPCベースのDVDメディア記録再生システ

ムのブロック図である。

【図 6】

この発明の第 1 の実施形態における DVD ドライブ 4 およびホスト 5 の処理の手順を説明するための略線図である。

【図 7】

この発明の第 2 の実施形態による PC ベースの DVD メディア記録再生システムのブロック図である。

【図 8】

この発明の第 3 の実施形態による PC ベースの DVD メディア記録再生システムのブロック図である。

【図 9】

この発明の第 3 の実施形態における DVD ドライブ 4 およびホスト 5 の処理の手順を説明するための略線図である。

【図 10】

この発明の第 4 の実施形態による PC ベースの DVD メディア記録再生システムのブロック図である。

【図 11】

この発明の第 4 の実施形態における DVD ドライブ 4 およびホスト 5 の処理の手順を説明するための略線図である。

【図 12】

この発明の第 5 の実施形態による PC ベースの DVD メディア記録再生システムのブロック図である。

【図 13】

この発明の第 6 の実施形態による PC ベースの DVD メディア記録再生システムのブロック図である。

【図 14】

この発明の第 6 の実施形態における DVD ドライブ 4 およびホスト 5 の処理の手順を説明するための略線図である。

【図 15】

この発明の第7の実施形態によるPCベースのDVDメディア記録再生システムのブロック図である。

【図16】

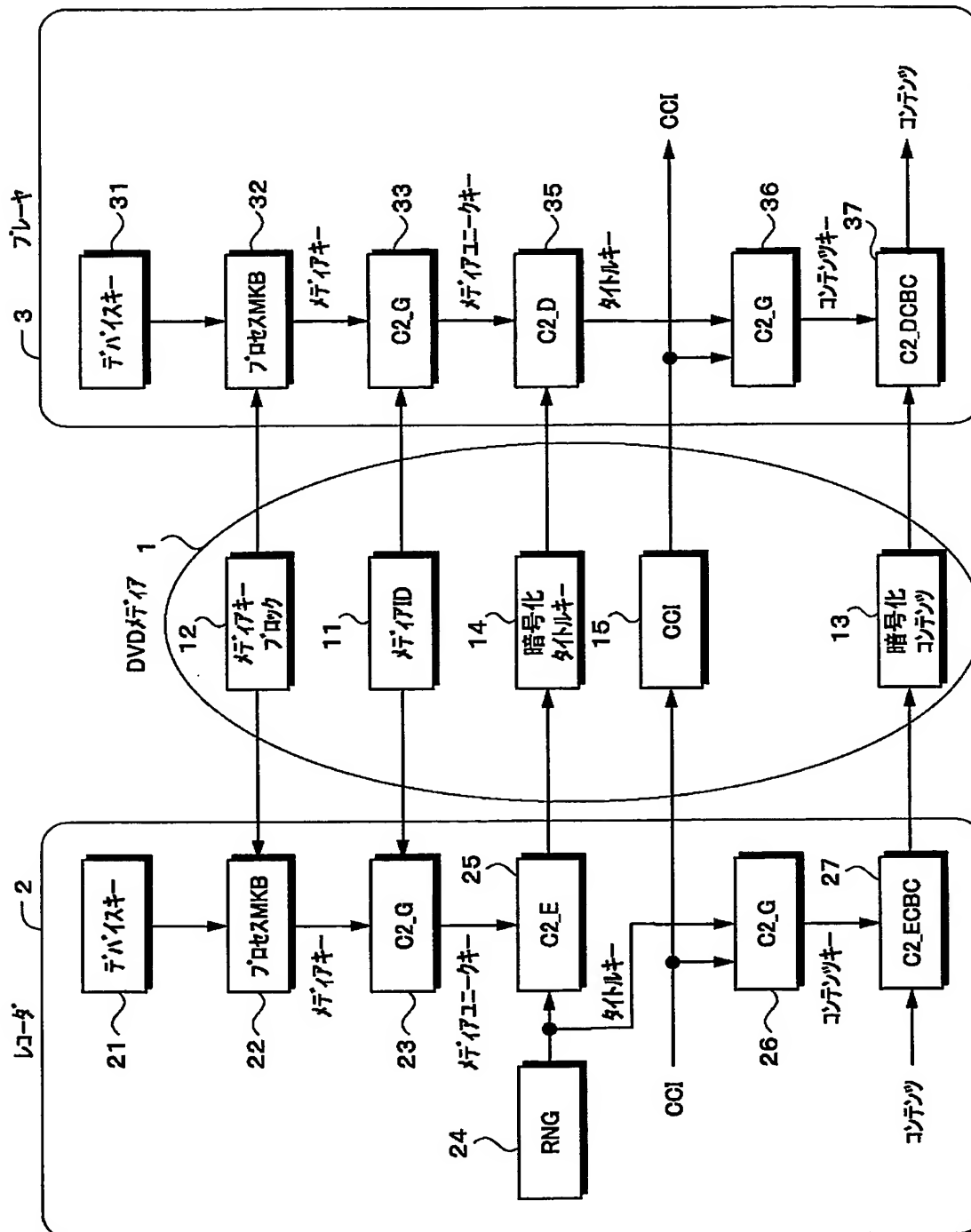
この発明の第7の実施形態におけるDVDドライブ4およびホスト5の処理の手順を説明するための略線図である。

【符号の説明】

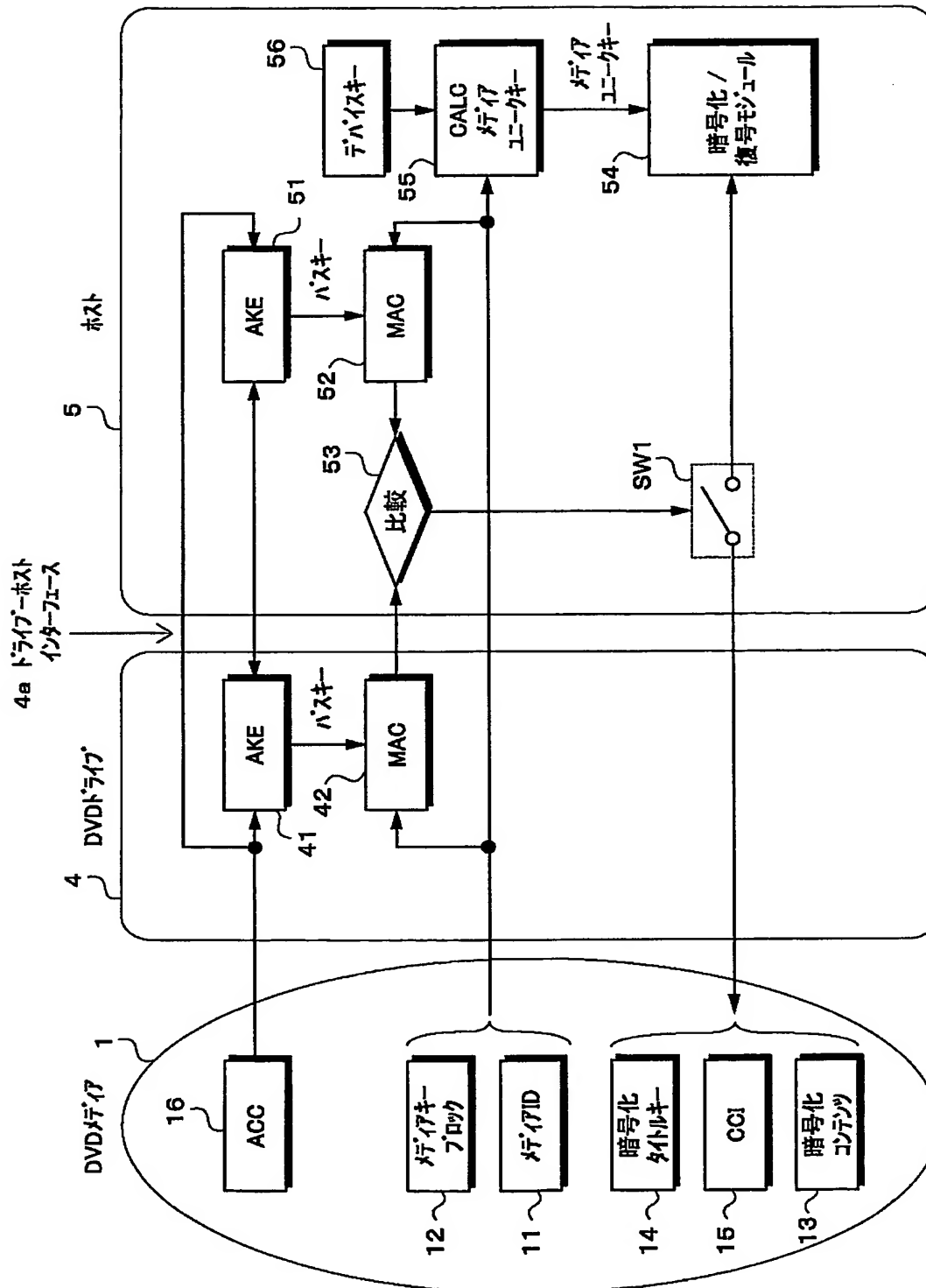
1・・・DVDメディア、2・・・レコーダ、3・・・プレーヤ、4・・・DVDドライブ、4a・・・インターフェース、5・・・ホスト、11・・・メディアID、12・・・メディアキープブロック(MKB)、13・・・暗号化コンテンツ、42, 52・・・MAC演算ブロック、46・・・デバイスキー、46a・・・デバイスキーの前半部、47・・・DESエンクリプタ、48・・・メディアユニークキー演算ブロック、49, 49a・・・DESエンクリプタ、49b・・・DESデクリプタ、53・・・MACを比較する比較、54・・・暗号化／復号モジュール、55・・・メディアユニークキー演算ブロック、56aデバイスキーの後半部、57・・・DESデクリプタ、58・・・デバイスキー合成部、59, 59a・・・DESデクリプタ、61・・・メディアユニークキー演算ブロック、62・・・パラメータA、63・・・暗号化／復号モジュール、64・・・パラメータB、65・・・DESエンクリプタ、66・・・DESデクリプタ

【書類名】 図面

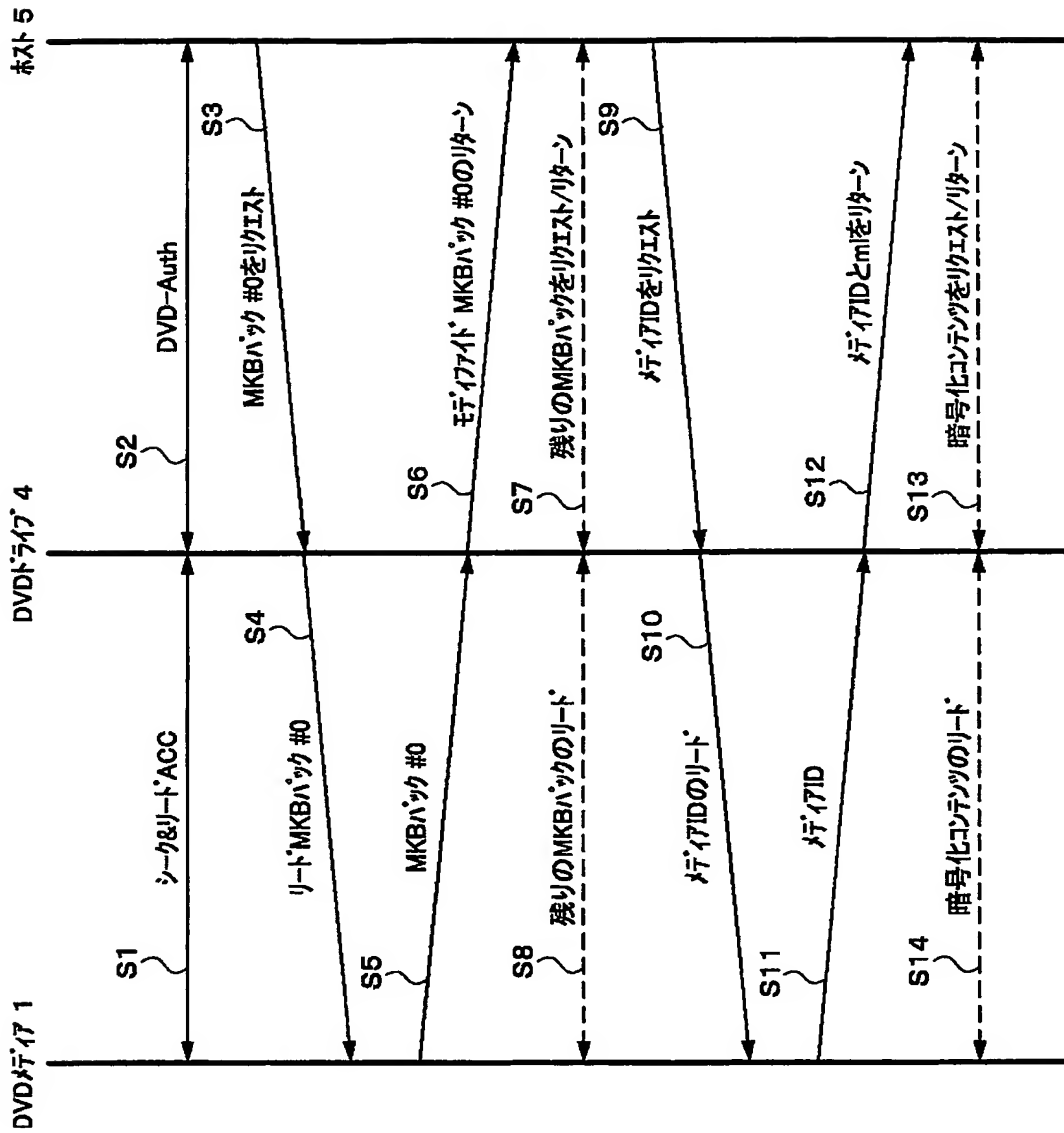
【図 1】



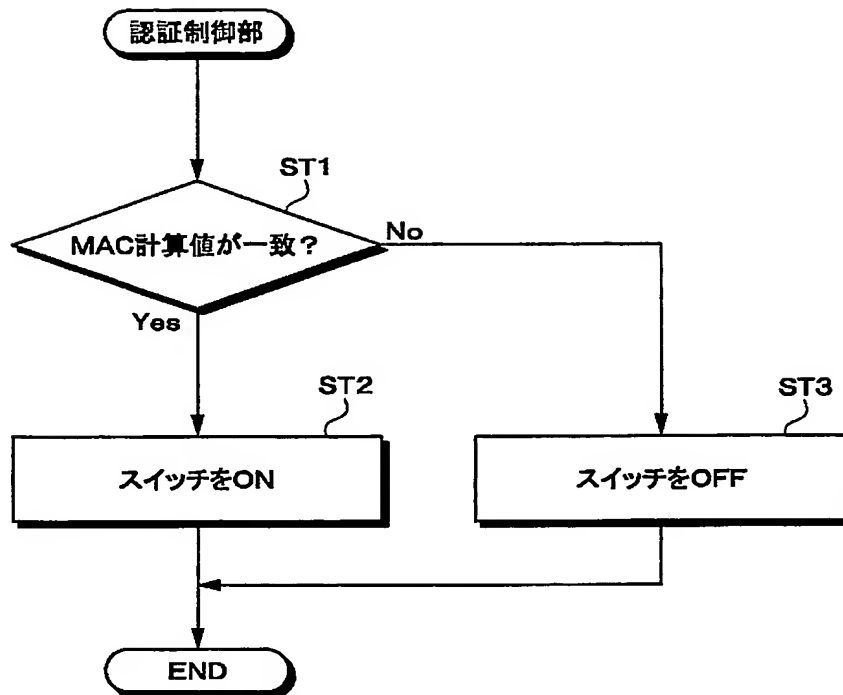
【図2】



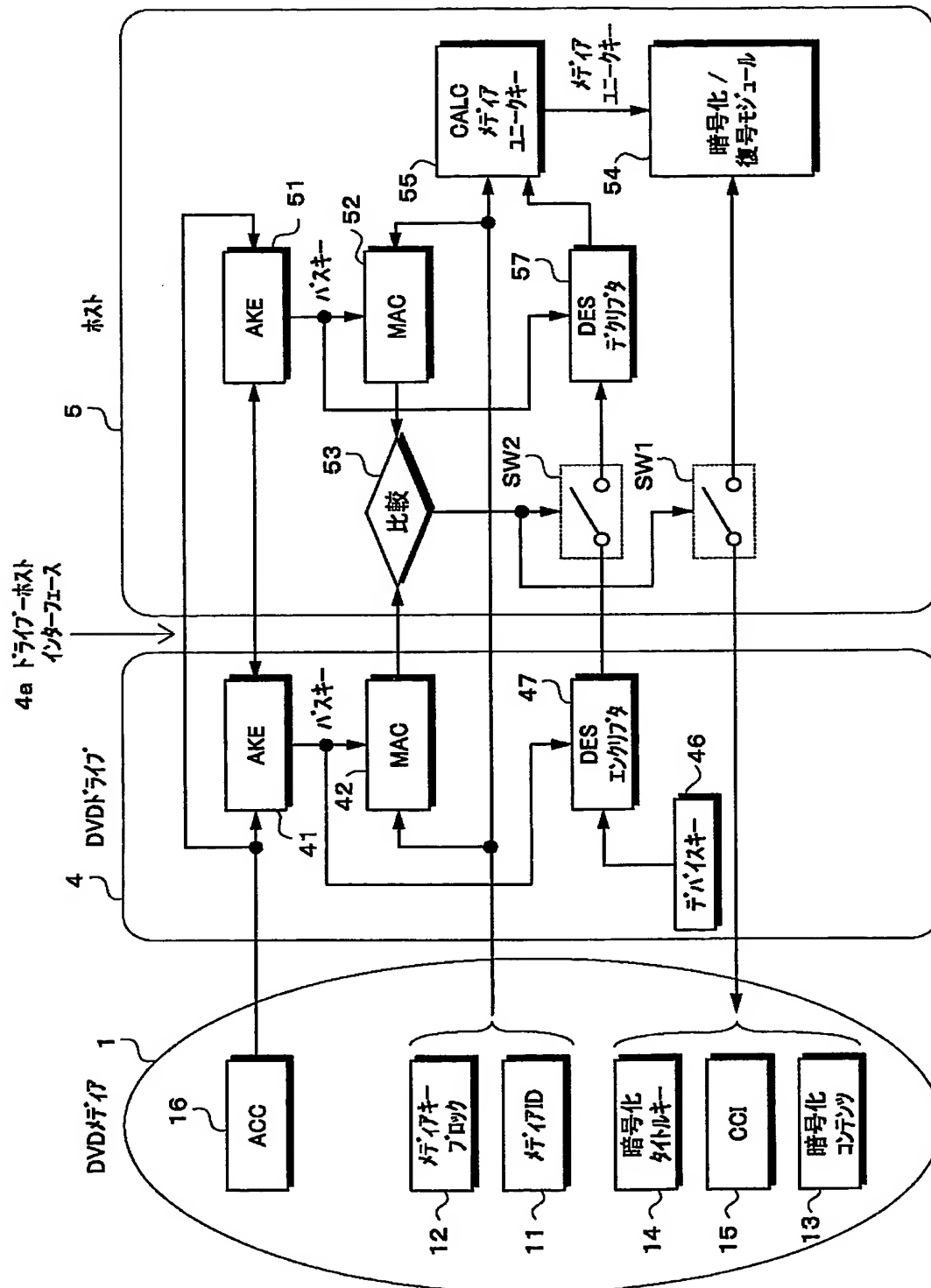
【図 3】



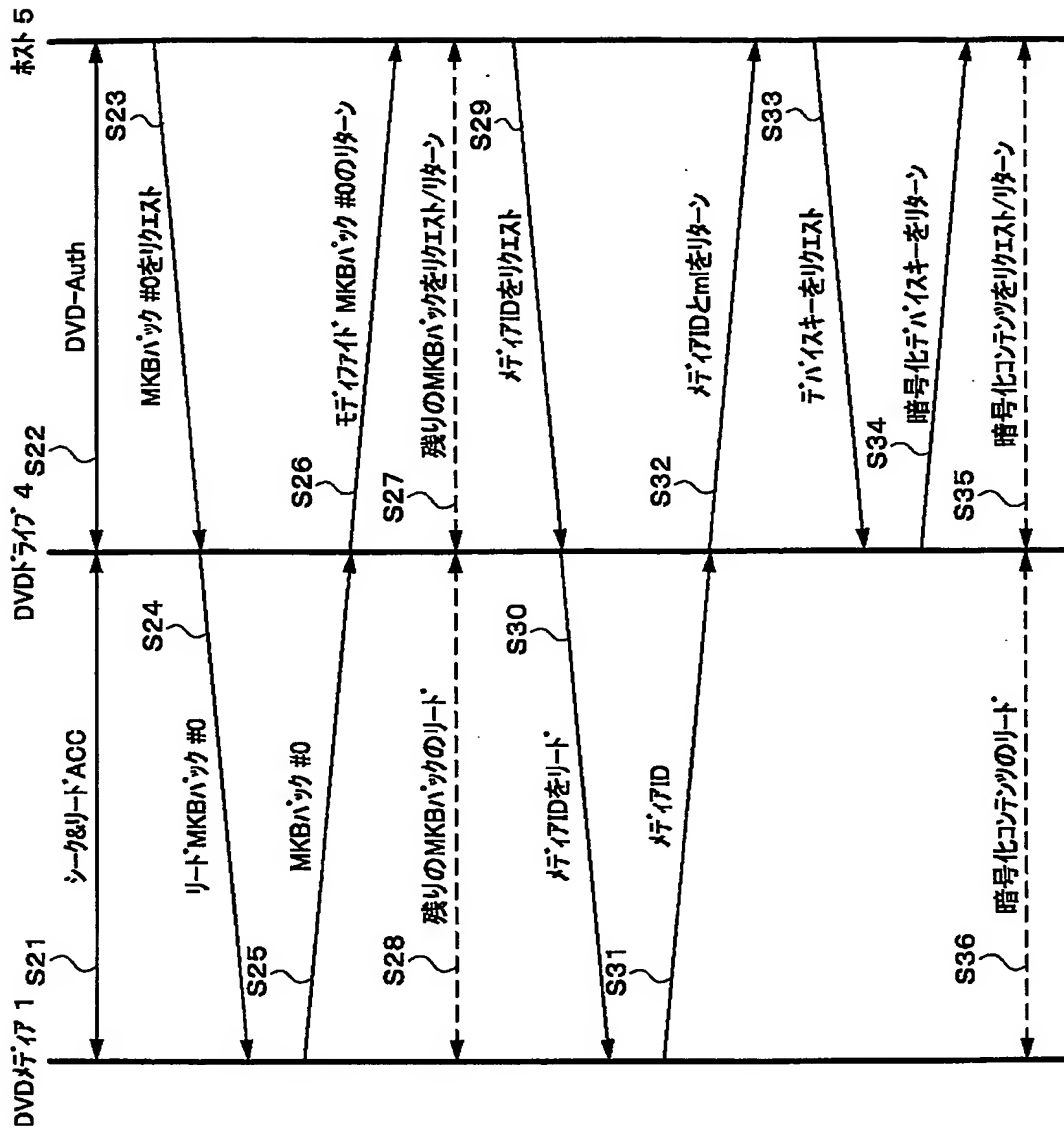
【図 4】



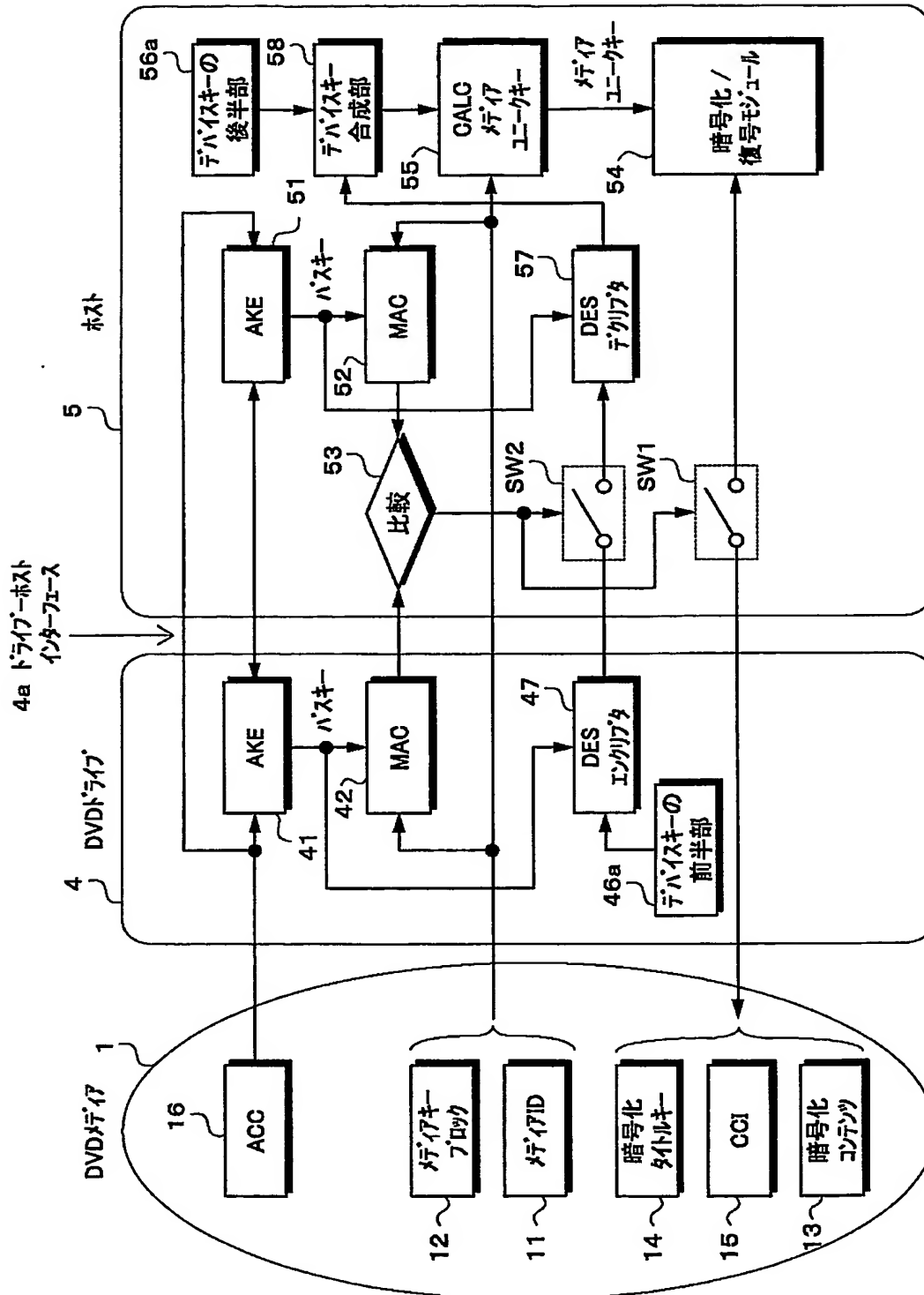
【図5】



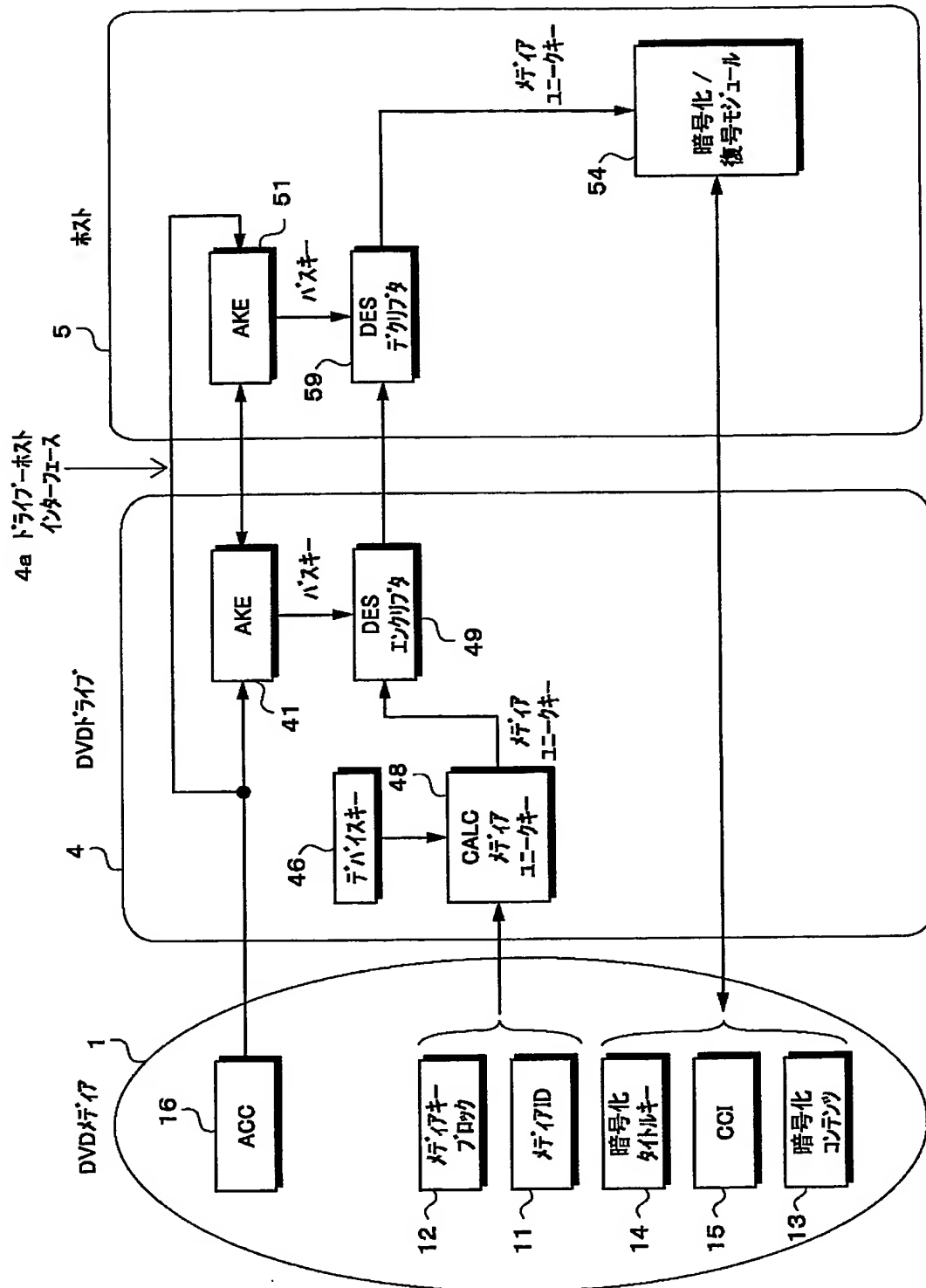
【図 6】



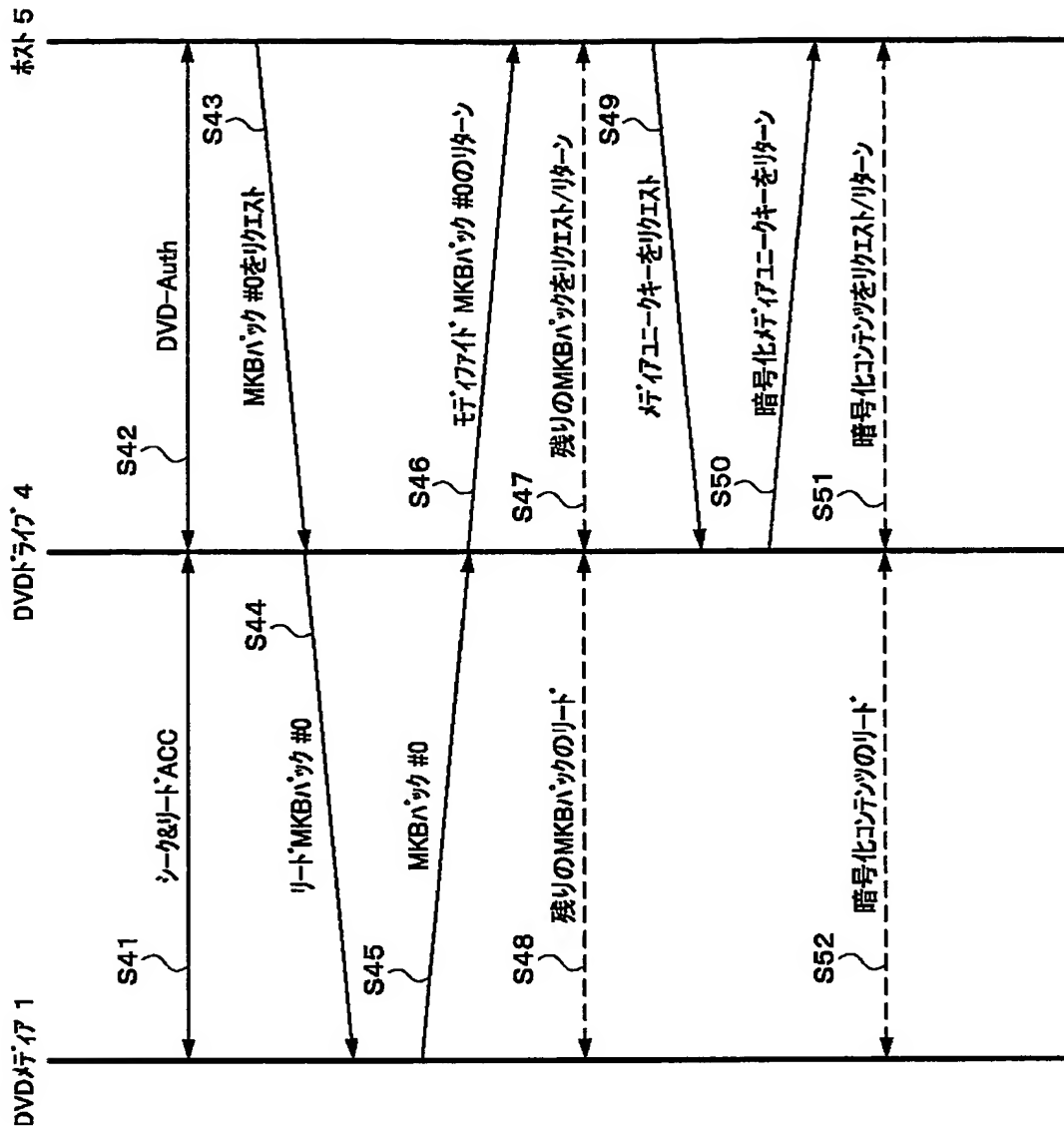
【図 7】



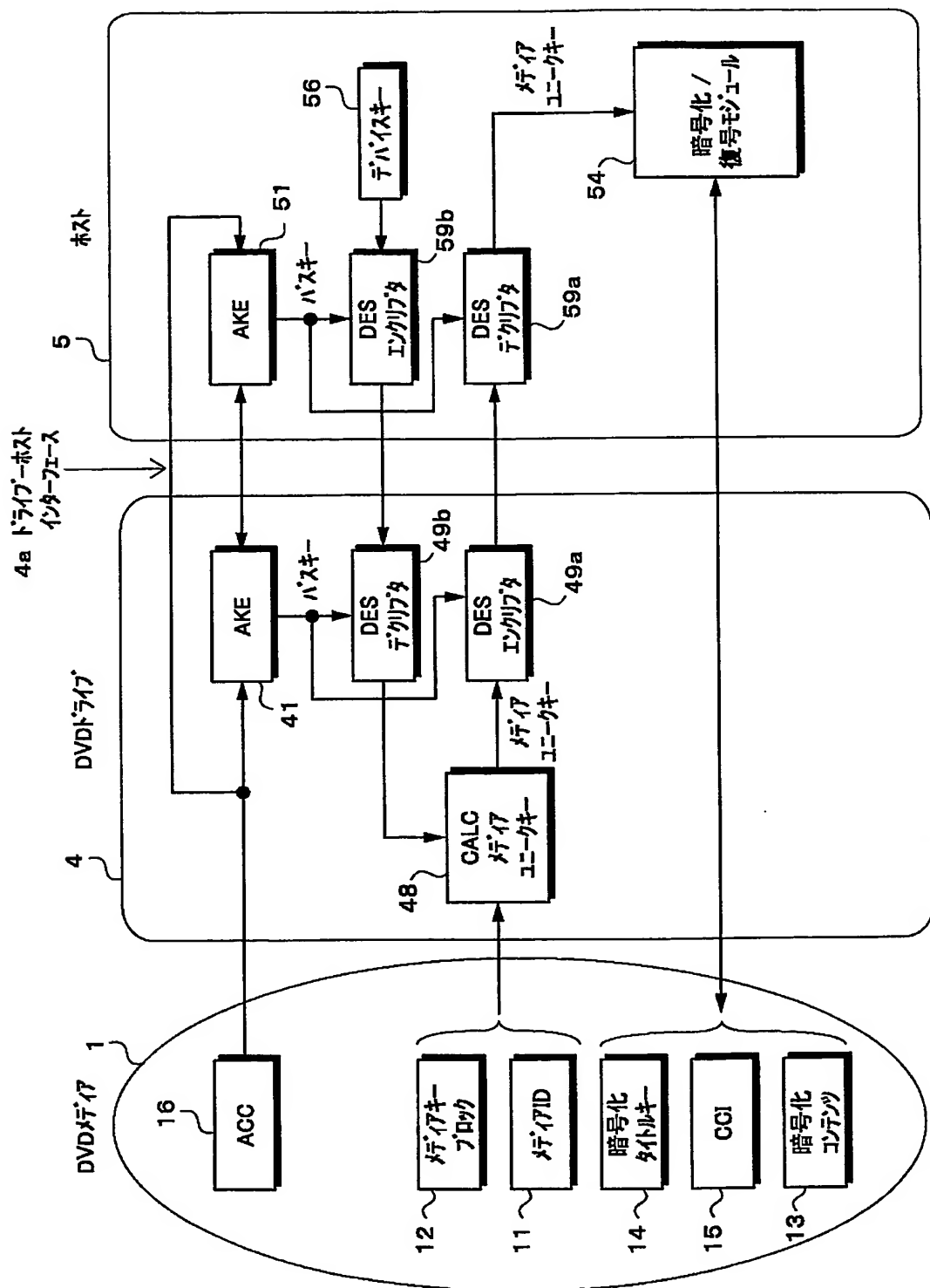
【図 8】



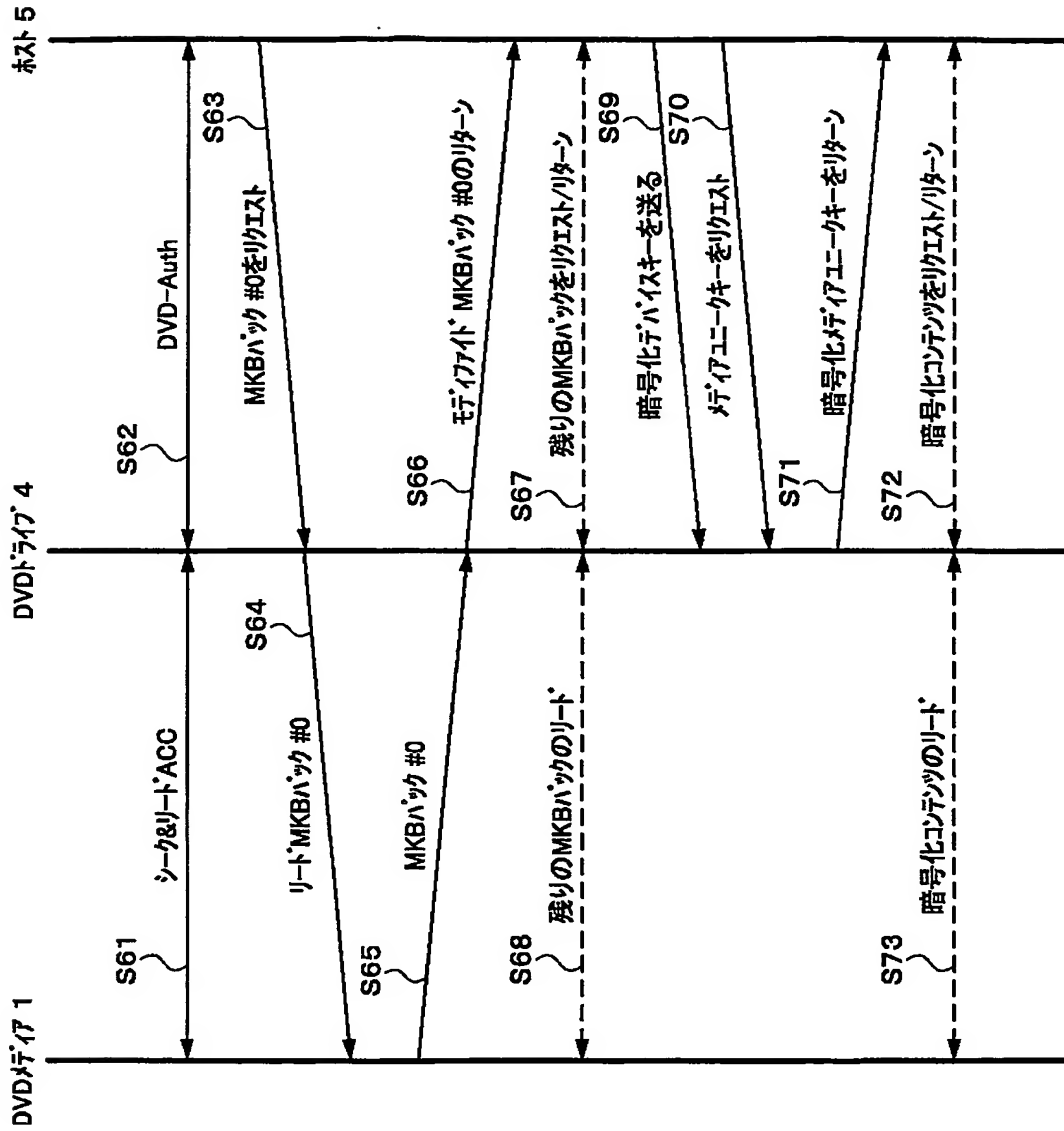
【図9】



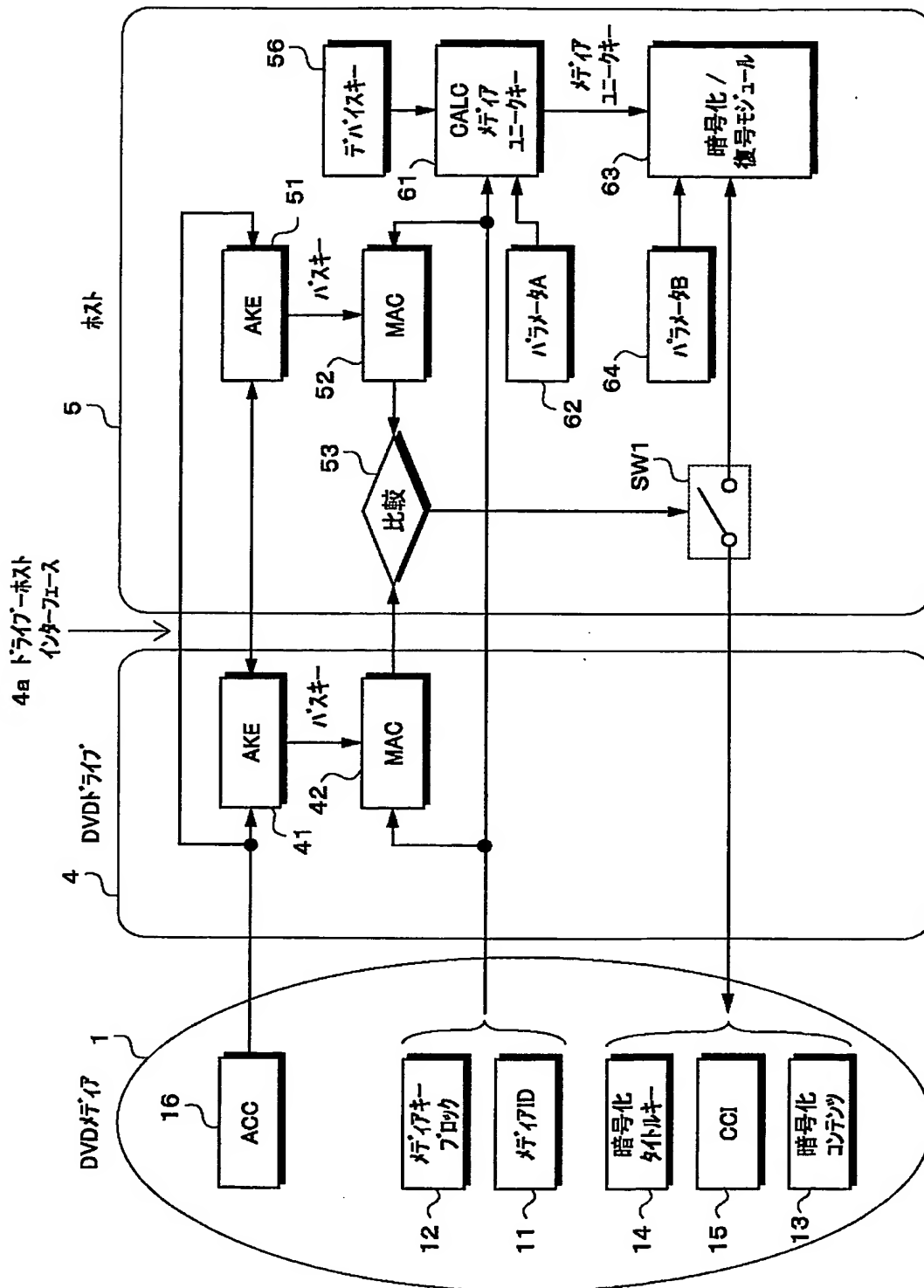
【図 10】



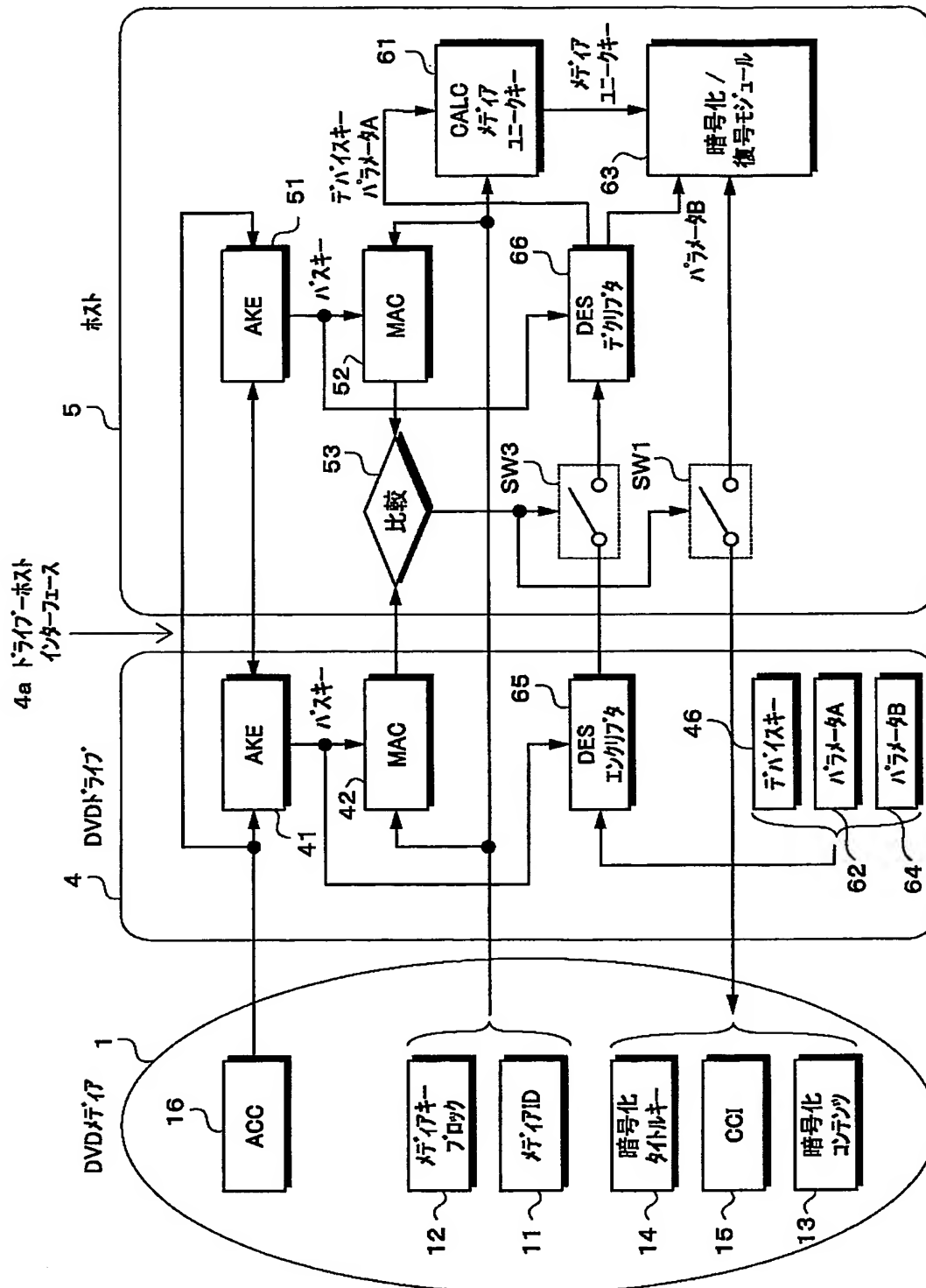
【図 11】



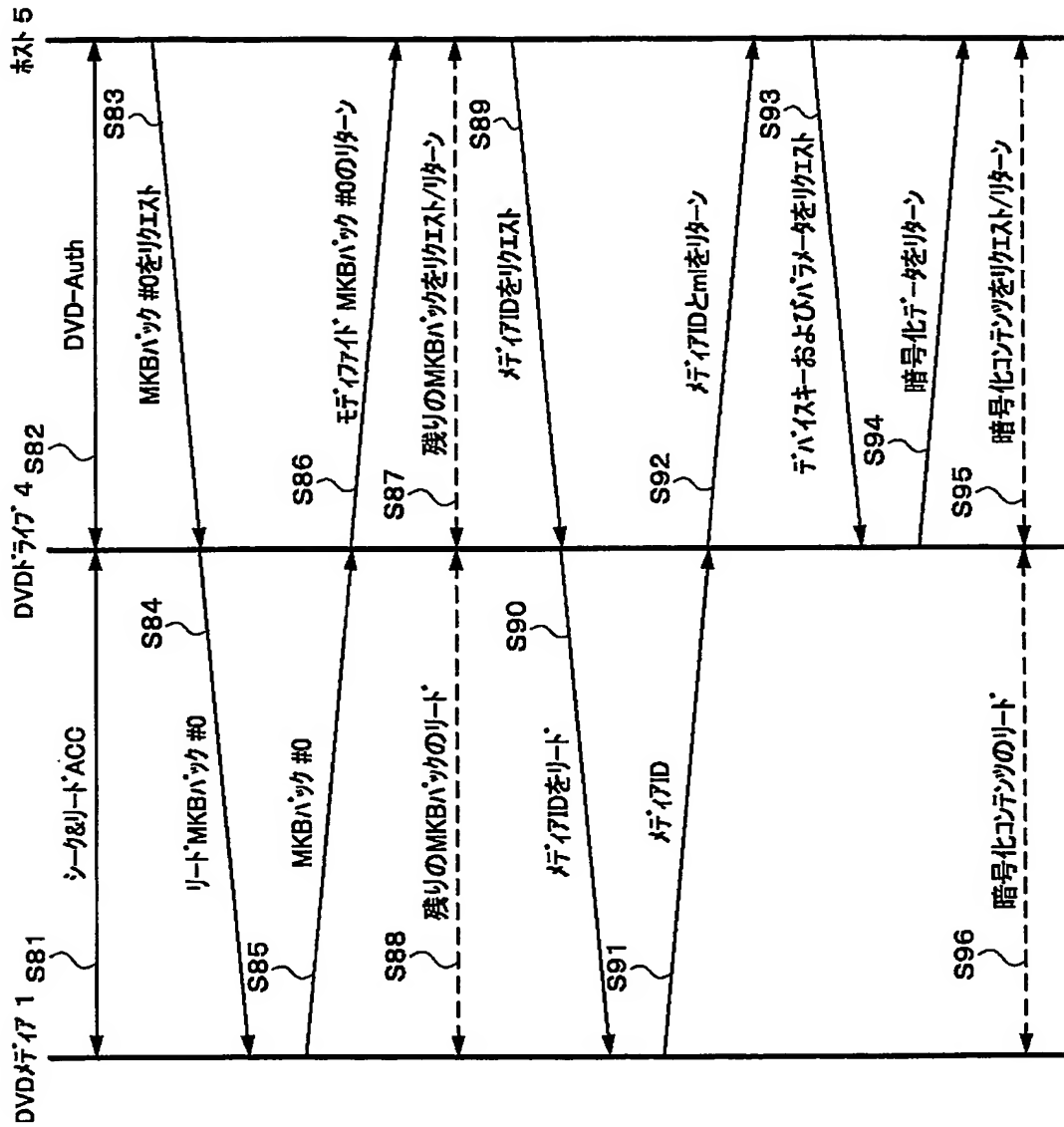
【図12】



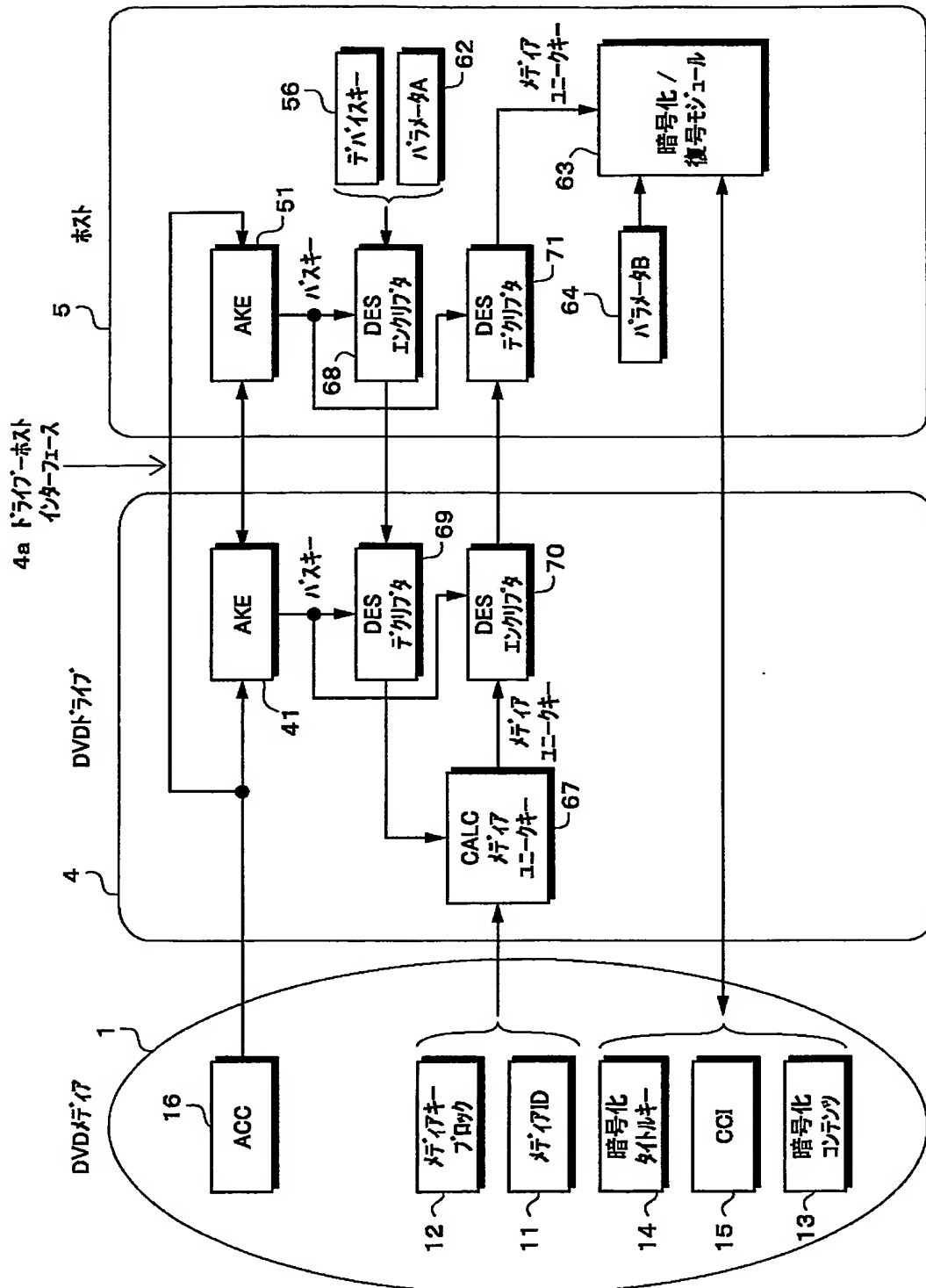
【図 13】



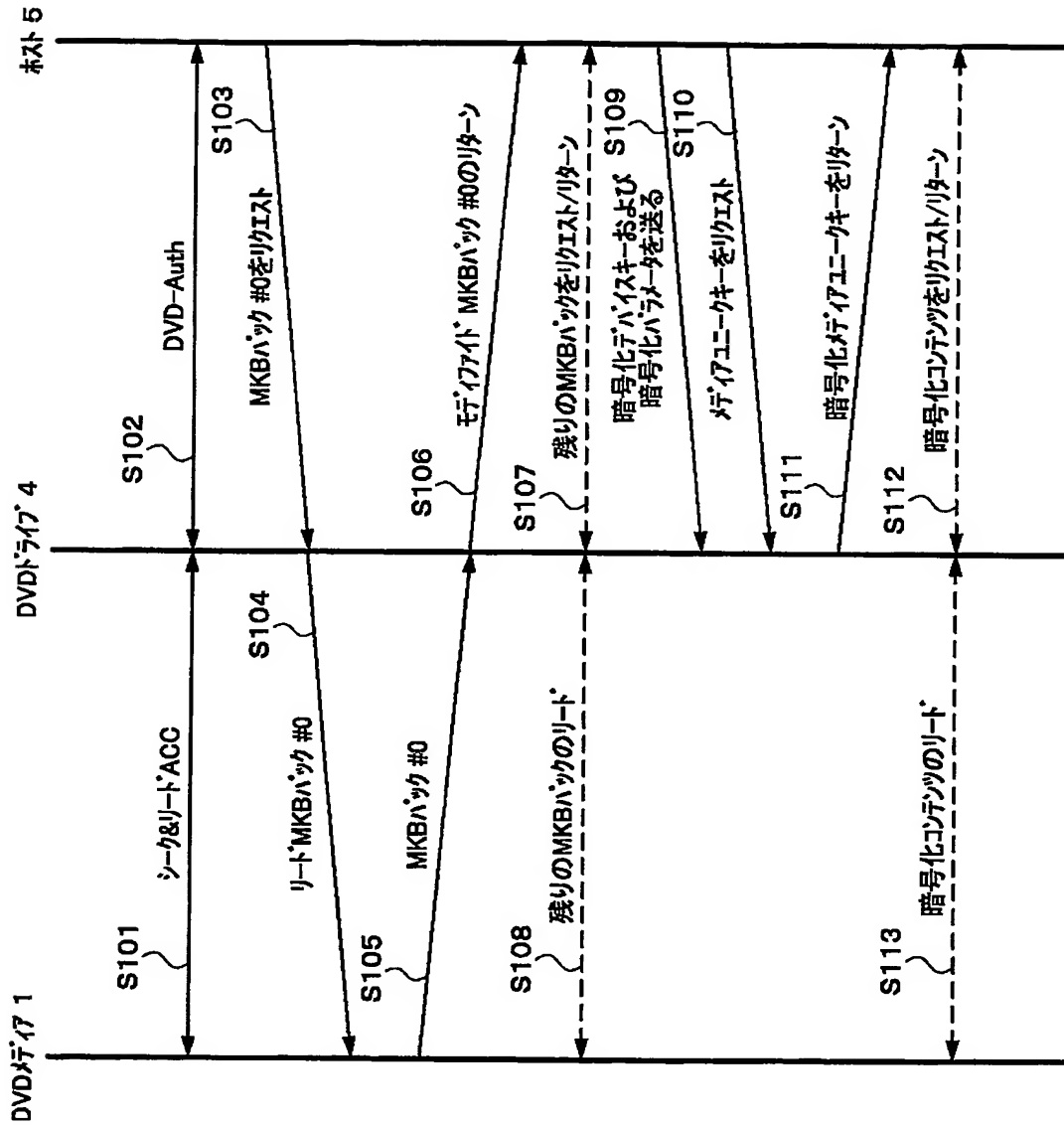
【図14】



【図15】



【図 16】



【書類名】 要約書

【要約】

【課題】 著作権保護技術の安全性を高め、また、違法なドライブ等の電子機器をリボークする。

【解決手段】 デバイスキー 46 がドライブ 4 側に実装される。デバイスキー 46 をセキュアにホスト 5 に伝送するために、デバイスキー 46 がバスキーで暗号化される。ホスト 5 側で、バスキーでデバイスキーが復号される。メディアユニークキー演算ブロック 55 が MKB 12 とメディア ID と復号されたデバイスキー 46 とからメディアユニークキーを演算する。演算ブロック 55 において、計算されたメディアキーが所定の値となる場合には、ドライブ 4 がリボークされ、処理が停止される。メディアユニークキーが暗号化／復号モジュール 54 に供給され、暗号化タイトルキー 14、CCI 15 からコンテンツキーが求められ、コンテンツキーを使用して暗号化コンテンツが復号され、記録されるコンテンツが暗号化される。

【選択図】 図 5

特願 2 0 0 2 - 3 5 5 1 1 4

出 願 人 履 歴 情 報

識別番号

[0 0 0 0 0 2 1 8 5]

1. 変更年月日

1 9 9 0 年 8 月 3 0 日

[変更理由]

新規登録

住 所

東京都品川区北品川 6 丁目 7 番 3 5 号

氏 名

ソニー株式会社